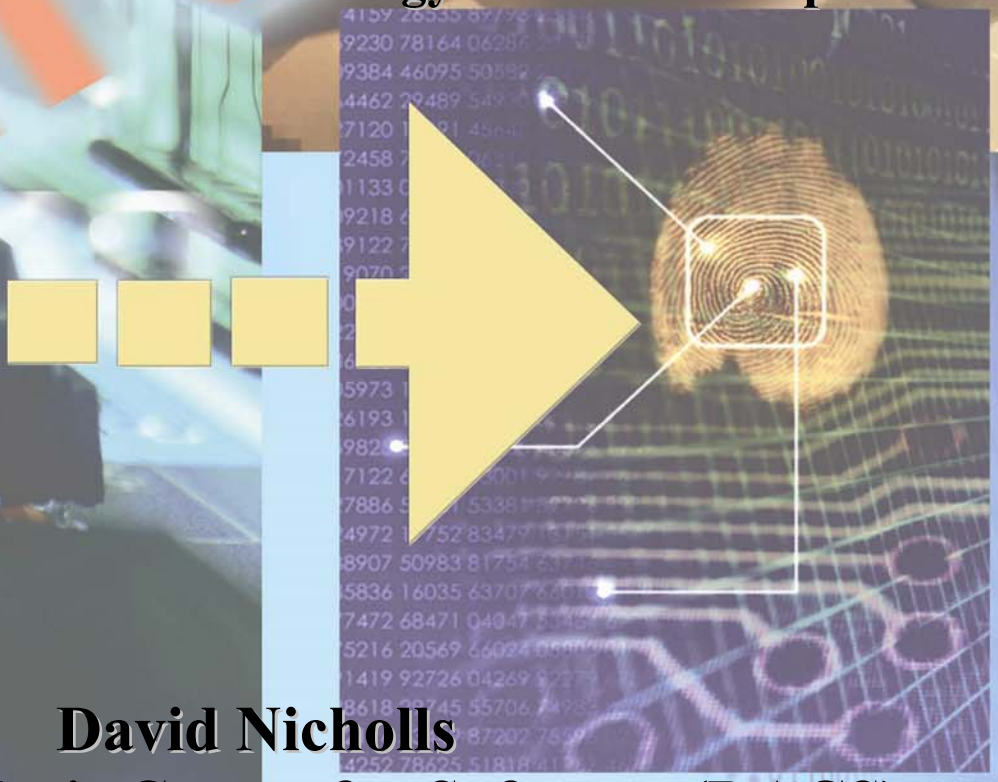
The Relevance of Y2K Lessons Learned to Critical Infrastructure Protection Initiatives

A DACS Critical Review/Technology Assessment Report



David Nicholls
Data and Analysis Center for Software (DACS)
775 Daedalian Drive
Rome, NY 13441-4909

Data and Analysis Center for Software

The Relevance of Y2K Lessons Learned to Critical Infrastructure Protection Initiatives

A DACS Critical Review/Technology Assessment Report

31 May 2002

Prepared by:
David Nicholls
Data and Analysis Center for Software (DACS)
775 Daedalian Drive
Rome, NY 13441-4909

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
31 May 2002	Technical Report	N/A

4. TITLE AND SUBTITLE

A Critical Review/Technology Assessment Report: The Relevance of Y2K Lessons Learned to Critical Infrastructure Protection Initiatives

5a. CONTRACT NUMBER
SPO700-98-4000

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
David Nicholls

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

ITT Industries
Advanced Engineering & Sciences (AES)
775 Daedalian Drive
Rome, NY 13441-4909

8. PERFORMING ORGANIZATION REPORT NUMBER

DACSCR/TA006

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)/AI
8725 John J. Kingman Rd.
Suite 0944
Ft. Belvoir, VA 22060

Air Force Research Lab/IFED
32 Brooks Rd.
Rome, NY 13440

10. SPONSOR/MONITOR'S ACRONYM(S)

DTIC-AI and AFRL/IFED

11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Available from: Data & Analysis Center for Software (DACS)
775 Daedalian Drive, Rome, NY 13441-4909
(800) 214-7921, CUST-LIASN@DACS.DTIC.MIL

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This CR/TA represents work performed by the Data and Analysis Center for Software (DACS) (Contract SPO700-98-D-4000) in support of the Office of the Deputy Under Secretary of Defense for Science and Technology (ODUSD(S&T)) over the calendar time period 12 May 1999 through 31 May 2002. This task was to provide support and analysis to the DoD in assessing the Year 2000 (Y2K) readiness of selected systems, and to provide support in reporting and analyzing Y2K End-to-End (E2E) testing plans, procedures, reports and results. After the Y2K rollover dates were successfully met, it was decided to extend the scope of the project to include Y2K lessons learned. A further refinement of the task scope was made to assess how Y2K lessons learned could benefit Critical Infrastructure Protection initiatives. The Y2K effort served as a model for how complex technological problems having high levels of interdependency and risk should be handled. As described in this report, there have been numerous lessons that have come out of the Y2K effort, from both government and industry, that need to be leveraged in order to adequately support critical infrastructure protection initiatives.

15. SUBJECT TERMS

Y2K, Lessons Learned, Critical Infrastructure Protection, Information Assurance, Cyber-terrorism

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Thomas McGibbon
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	183	19b. TELEPHONE NUMBER *(include area code)* 315-334-4900

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

PREFACE

This Critical Review/Technology Assessment represents work performed by the Data and Analysis Center for Software (DACS) (Contract SPO700-98-D-4000) in support of the Office of the Deputy Under Secretary of Defense for Science and Technology (ODUSD(S&T)) over the calendar time period 12 May 1999 through 31 May 2002. The report represents the culmination of efforts performed under DACS Technical Area Task (TAT) 19, CLIN 0002 Delivery Order 0018 (DA-99-0010/0024) entitled "ODUSD(ST) Y2K Analysis and Support".

This task was awarded to the DACS to provide support and analysis to the Special Assistant for Computing and Software Technologies, Office of the Deputy Under Secretary of Defense (Science and Technology) (SACST/ODUSD(S&T)) in assessing the Year 2000 (Y2K) readiness of selected systems within the Service Laboratories, High Performance Computing Centers (HPCCs) and Department of Defense (DoD) Modeling and Simulation (M&S) programs, and to provide the necessary support needed in reporting and analyzing Y2K End-to-End (E2E) testing plans, procedures, reports and results.

After the Y2K rollover dates were successfully met, it was decided to extend the scope of the project to include Y2K lessons learned. A further refinement of the task scope was made to assess how Y2K lessons learned could benefit Critical Infrastructure Protection initiatives.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This task was originally undertaken by the Data and Analysis Center for Software (DACS) to provide support and analysis to the Special Assistant for Computing and Software Technologies, Office of the Deputy Under Secretary of Defense (Science and Technology) (SACST/ODUSD(S&T)) in assessing the Year 2000 (Y2K) readiness of selected systems within the Service Laboratories, High Performance Computing Centers (HPCCs) and Department of Defense (DoD) Modeling and Simulation (M&S) programs, and to provide the necessary support needed in reporting and analyzing Y2K End-to-End (E2E) testing plans, procedures, reports and results. The successful completion of the Y2K rollover extended the focus of the study to allow the collection and analysis of lessons learned from the Y2K experience as they applied to general Information Technology (IT) processes, and as they could be leveraged to support ongoing U.S. Government Critical Infrastructure Protection (CIP) initiatives to ensure cyber-security.

Research of the literature and the Internet yielded a wealth of information pertaining to lessons learned from within DoD and the Services, as well as from organizations outside of DoD whose lessons learned could be considered appropriate to address growing concerns over critical infrastructure issues. The tragic events of September 11, coupled with previous and subsequent hacker and virus/worm attacks on DoD, Government and commercial Internet sites, helped to drive home the point that a concentrated effort was, and is, mandatory to develop an intensely focused and comprehensive strategy to protect the U.S. information infrastructure from intentional and unintentional hacking, as well as premeditated cyber-attacks from terrorists and/or unfriendly governments and organizations.

This CR/TA, then, is structured to address:

SECTION 2: The technical challenge associated with the Year 2000 problem

SECTION 3: The plans developed to help meet that challenge

SECTION 4: How those plans were implemented

SECTION 5: What occurred as a result of the Y2K rollover

SECTION 6: The lessons learned from Y2K

SECTION 7: How those lessons learned apply, should apply, or have not been applied to critical infrastructure protection issues

SECTION 8: Summary and conclusions

In addition, Appendices have been added to provide additional insight into the worldwide events that were reported during the Y2K rollover (Appendix A); a list of acronyms used throughout this report (Appendix B); a list of resources available on the Internet (with provided links) that relate to Y2K and Critical Infrastructure Protection issues (Appendix C); a comprehensive list of bibliographic references that were obtained and reviewed as part of this effort (Appendix D); and several appendices that contain lists of reports available through the U.S. General Accounting Office (GAO) that pertain to Y2K and critical infrastructure protection. These GAO appendices were compiled based on keyword searches at the GAO website (www.gao.gov). The search terms used were "Year 2000 Computing Challenge" (Appendix E), "Year 2000 Computing Crisis" (Appendix F), "Critical Infrastructure Protection" (Appendix G), "Information Security" (Appendix H), "Defense Computers" (Appendix I), and "Computer Security" (Appendix J).

To facilitate additional research that readers may want to pursue, the hardcopy of this CR/TA is accompanied by a PDF version of the report on CD-ROM. The list of resources (Appendix C), the bibliographic citations (Appendix D) and the GAO report references (Appendices E through J) are extensively hyperlinked to their source on the Internet, as well as the status of the link (i.e., active or inactive) as of a specific date. The links for the GAO reports should all be considered active as of 15 March 2002.

2 The Challenge

The origin of the Year 2000 problem is based in the 1950's and 1960's. Programmers, in order to reduce the need for expensive computer memory, used the convention of storing dates using two digits, rather than four, for the year. They assumed that the software would be replaced long before the year 2000 and did not anticipate that these legacy systems would survive until then. In the transition to the year 2000, it was suspected that systems based on the use of two digit dates would produce incorrect results, or fail altogether, if they could not determine whether "00" represented the year 2000 or 1900. Identifying the systems that would be affected, the systems that interfaced with affected systems, the impact of failure of these systems, and how to correct both the affected and interfacing systems, presented an enormous management and technical challenge.

It was anticipated that, although there were several Y2K rollover dates that would need to be addressed, the most critical and most widely publicized problems would appear on the following dates:

- 31 December 1999 to 1 January 2000
- Leap Year Dates: 28 February 2000 to 29 February 2000 and 29 February 2000 to 1 March 2000

The Y2K problem was especially critical to the Department of Defense because of its dependence on computers and information technology for its military advantage. Of the Departments in the Federal Government, the DoD was identified as having the largest number of computer systems. These included weapons systems, command and control systems, satellite systems, inventory and transportation management systems, and payroll and personnel records. As a result, the Year 2000 problem was recognized as an especially large, complex and insidious threat to the DoD. The stated goal of the DoD in addressing this threat was:

"To ensure the continuance of a mission-capable force able to execute the National Military Strategy before, on, and after January 1, 2000, unaffected by the failure of mission-critical or

support systems to properly execute date-related information." *– Department of Defense Year 2000 Management Plan, Version 2.1, September 1999*

The DoD recognized that it needed to:

- identify all potential Y2K risks and threats to the continuity of its operations
- take decisive action to mitigate those risks
- develop contingency plans to continue operations if failures were to occur

As such, the DoD Year 2000 Office established the following specific objectives to ensure that the Department attained its stated goal:

- Ensure that all DoD systems with Y2K vulnerabilities were fixed, replaced or terminated
- Ensure that all DoD milestones were met and all reporting requirements to the Office of Management and Budget (OMB) and Congress were satisfied
- Ensure that DoD Y2K activities were adequately coordinated within DoD and with other Federal agencies; state and local government agencies; suppliers; the private sector; foreign allies; coalition partners; and other countries
- Identify all issues that could not be resolved by individual DoD Components and ensure resolution at the appropriate level in DoD
- Ensure testing was conducted to validate that systems were Y2K compliant and still performed as intended
- Ensure contingency plans were developed and technical solutions were tested and confirmed to be effective
- Ensure that the capability existed to coordinate activities required by the President's Council on Year 2000 Conversion before, on and after January 1, 2000

3 The Plan

In response to the Y2K challenge, the DoD developed and implemented the "DoD Year 2000 (Y2K) Management Plan". The document applied to all DoD Components, including the Office of the Secretary of Defense (OSD), Military Departments, Chairman of the Joint Chiefs of Staff, Combatant Commands, Inspector General of the Department of Defense, Defense Agencies and DoD Field Activities. The plan outlined the DoD's systematic approach to Y2K remediation and management for the more than 9,900 systems of the DoD (of which almost 24 percent, or 2,367 systems, were ultimately categorized as active mission-critical). It presented the management approach, planning strategy, policy, and actions that the DoD would use to address the Y2K challenge. Compliance to Y2K requirements was to be ensured from three perspectives, (1) individual system renovation and certification, (2) functional-centric and (3) mission-centric. Individual developers/owners were to perform the system renovation, certification and implementation tasks. The Principal Staff Assistants (PSAs), Commanders-in-Chief (CINCs), Services and Agencies were responsible for ensuring that functional-centric testing was performed. The Joint Staff was chartered to work with the CINCs worldwide to conduct joint operational evaluations (mission-centric) aimed at verifying Y2K compliance and ensuring continuity of operations at and beyond the critical rollover dates. Selected reviews were to be performed by the DoD audit/inspection community.

The plan recognized that there were four critical resources that each Component needed to manage effectively to successfully meet the Y2K challenge:

- Leadership
- Time
- Money
- Skilled personnel

It noted that existing resources would be used for Y2K compliance efforts. Resources were to be reallocated/reprogrammed to address the need and were to be applied to mission-critical systems before being allocated to non-mission-critical systems. Software enhancements, preplanned product improvements, and changes to nonessential software were to be postponed until all Components' systems were assessed, renovated, and verified as Y2K compliant.

As noted above, mission-critical systems were to receive priority for all Y2K repair, testing, certification and replacement activities. Mission-critical systems included those:

- defined by the Information Technology Management Reform Act (Clinger-Cohen Act) as National Security Systems (NSS), i.e., Intelligence Activities; Cryptologic Activities related to National Security; Command and Control of military forces integral to a weapon or weapon system; and systems critical to direct fulfillment of military or intelligence missions
- identified by the CINCs which, if not functional, would preclude the CINC from conducting missions across the full spectrum of operations
- required to perform Department-level and Component-level core functions

Systems deemed to be non-mission-critical were divided into two categories:

- Mission-essential: The loss of those functional or tangible capabilities and assets that, if left uncorrected, would have an adverse impact on the overall mission functionality, i.e., eventual degradation and loss of mission capability
- All other non-mission-critical systems were to be tracked by Services and Agencies as deemed appropriate

DoD Y2K compliance, as outlined in the plan, was to be achieved through repair, replacement, or termination. The management strategy emphasized centralized policy planning and decentralized implementation and execution. This strategy allowed each DoD Component the maximum flexibility to implement solutions on a system-by-system basis.

The first step in determining the priorities for the focus of the Y2K effort was to place information systems in the broader context of their supported function(s). For the DoD mission areas, the Joint Staff and the CINCs were given responsibility for identifying and prioritizing the DoD's critical missions. PSAs were to be given specific responsibility to oversee Y2K compliance of critical supporting functions.

Once the critical missions and functions were identified and prioritized, the underlying information systems were to be identified in the context of specific mission threads. The ***interdependencies*** between systems were also required to be identified in order to allow decision-makers to view information systems in the context of their contribution to achieving the DoD operational goals. DoD Components were to be tasked with identifying the interdependencies between and within systems, and were to determine workarounds and alternatives for any identified system which could not be made compliant within the schedule constraints such that DoD critical missions and functionality would not be compromised.

The DoD Components and PSAs were given responsibility for reporting on all systems under their programmatic control, providing the Y2K status of each critical system, including current implementation status and plans; results of system certification testing; schedules for fielding, refurbishment, replacement; etc. The DoD Deputy Chief Information Officer (CIO) was tasked with maintaining the DoD "enterprise-wide" view by capturing evolving system Y2K status in the context of critical missions and functions, support functions, system interdependencies and programmatics using the OSD Y2K database. This database was to be the single official reporting source to support senior management and the regular Office of Management and Budget reports. The database was to be loaded and updated on a regular cycle in an automated process from the reporting agencies' local databases and/or updated interactively online through a provided, secure web interface. The Joint Staff, Services, CINCs, Agencies and PSAs were to be held accountable for the quality and completeness of their data maintained in the OSD Y2K database.

The CINCs were assigned the responsibility of conducting operational evaluations to identify specific Y2K problems, to establish workarounds where feasible, and to propose alternative or contingency approaches to ensure uninterrupted critical-path operations. In addition, the PSAs and the Services were to conduct functional end-to-end tests to ensure continuity of all critical support functions, such as logistics, finance, et. al., and to work directly with the CINCs to determine where these functional operations would mesh with critical mission threads. The data resulting from these evaluations and end-to-end tests were to be maintained in the OSD Y2K database, along with all relevant information about each system in the thread.

The functional areas designated by the DoD for end-to-end testing included:

Communications:	Telecommunications and other systems used to transmit and receive information
Logistics:	Management of material, operation of supply, maintenance activities, material transportation, base operations and support
Health/Medical:	Providing medical care to active military personnel, dependents and retirees
Personnel:	Recruitment of new personnel, personnel relocation, civilian disability compensation, veterans education assistance, etc.
Intelligence:	Collection, processing, integration, analysis and interpretation of available information concerning foreign countries or areas

Assessments of Y2K readiness were to include mission dependencies of all critical systems, including any support systems that were essential to critical-path operations. The Y2K database was to be used to integrate the status of individual systems, the results of function-centric evaluations, and the results of mission-centric CINC assessments into an "enterprise-wide" context to determine and prioritize needs and solutions.

Y2K Operational Readiness exercises were to be selected, conducted and evaluated by the Joint Staff in accordance with the Joint Year 2000 Operational Evaluation Plan. During these evaluations, only Y2K-compliant systems were to be tested. Operational Contingency Plans (CPs) were to be used in lieu of non-compliant or dysfunctional systems in order to complete essential mission/functional end-to-end testing. Results from these exercises were to be reported to the DoD Y2K Office and the Y2K Steering Committee, and were to be used to determine the level of confidence in DoD Y2K mission capabilities.

The DoD Components and PSAs were to be responsible for the timely implementation of all Y2K remedies, reporting the implementation results and mission and function status to the DoD Deputy CIO who would, in turn, monitor ongoing progress.

DoD Y2K operational readiness reporting to the DoD Y2K database was to be performed by all individual program managers, as well as their Service or Agency Y2K offices. Scorecards would then be generated for each functional area and presented at the Y2K Readiness Reviews. In addition, the Joint Staff (JS)/CINC Operational Exercise and Functional E2E test planners would provide status information to the DoD Y2K database regarding any "thin threads" or segments identified for testing. The information was to be made available for subsequent analysis and assessment at all appropriate levels of the DoD.

Finally, DoD was to conduct a series of Y2K Table Top Exercises (TTE) to guide and support OSD and Component decision makers to collectively contemplate the implications of managing a National Security contingency coincident with the Y2K situation. The TTE activities would include participation in the planning and execution of inter-departmental Y2K exercises under the direction of the Executive Office of the President. The TTE activities were to include the following:

- **Y2K Functional Seminars and Functional Policy Workshop:** A set of three functionally oriented one-day seminars to serve as a prelude to subsequent DoD-level and National Y2K Table Top Exercises. Intended to be informational in

nature, they would address functional and cross-functional policy implications of the Y2K environment on mobilization, deployment, employment and sustainment capabilities. Participants were to include the appropriate Under Secretaries of Defense, Assistant Secretaries of Defense, Principal Staff Assistants, and key leadership from the Joint Staff, Services and Defense Agencies.

- **DoD Level Y2K Table Top Exercise:** This one-day, facilitated exercise was to focus on policy and crisis management in response to a National Security emergency. It required full participation by Principals, including the Deputy Secretary of Defense, Vice Chairman Joint Chiefs of Staff, the Service Secretaries, the DoD CIO, selected Principal Staff Assistants, and Defense Agency Directors.

- **National Level Y2K Table Top Exercise:** This Principle level activity, which was to be planned by the White House Y2K Office, was to focus on national contingency policy review and associated decision making. The DoD CIO was to provide support to the White House and provide assistance in coordinating the activities of other Federal agencies participating in the national exercise.

3.1 The Five-Phase Management Process

As previously mentioned, the DoD's Y2K management strategy was to follow the fundamental DoD precept of centralized policy and decentralized implementation and execution, thereby allowing each DoD component to exercise the maximum flexibility to implement appropriate solutions.

The DoD used the Federal Government-wide five-phase management process for Y2K that had been stipulated by the Office of Management and Budget. Table 1 identifies these phases, as well as the original target dates for completion of each phase.

Table 1: Y2K Five-Phase Management Process

Phase	Objectives	Target Completion Dates	
		Mission-critical	All Others
Awareness	Promote Y2K awareness across the entire organization, and at all levels of leadership	31 Dec 1996	31 Dec 1996
Assessment	Inventory all systems; identify mission-critical systems; assess each for Y2K risks and issues; develop strategy to address each risk; prioritize all systems for fixing; and develop contingency plans	30 June 1997	30 June 1997
Renovation	Repair, replace or terminate systems to ensure Y2K compliance	30 June 1998	30 Sept 1998
Validation	Test systems and provide appropriate certification for Y2K compliance	30 Sept 1998	31 Jan 1999
Implementation	Fully deploy all renovated and replacement systems	31 Dec 1998	31 Mar 1999

The Awareness phase focused on promoting Y2K awareness across DoD at all levels of leadership. The Assessment phase was used to inventory all systems, identify mission-critical systems (assessing each for Y2K risks and issues), prioritize all systems for fixing, and develop contingency plans. The Renovation phase focused on replacing, repairing, or terminating systems to ensure Y2K compliance. The Validation phase tested systems for Y2K compliance. And finally, renovated systems were deployed during the Implementation phase. Not every system went through all five phases. The process followed a very aggressive schedule in order to meet the fixed 1 January 2000 deadline.

Figure 1 provides an overview of the Five-Phase Management Process that was used by the DoD to address the Y2K problem. Table 2 includes the exit criteria that were defined for each phase of the process.

The DoD considered obtaining leadership focus as the key to success in the ***Awareness*** phase, as leadership must understand the size, pervasiveness and scope of the Y2K problem, prepare the necessary plans, and re-focus and prioritize their organizational missions to attack the problem. Each Component's leadership was expected to decide the level of resources and attention that would need to be allocated to defining and implementing Y2K solutions. To this end, the DoD Year 2000 Management Plan defined the first step in attacking Y2K as the establishment of a Component-level Y2K Office and a senior point of contact that could (1) understand the technical issues associated with Y2K and (2) work closely with the Service Chief or Agency Head to develop a Component-wide strategy and approach to successfully manage their Y2K effort. Key to the success of theY2K process was:

"All participants…must understand the need to collect and disseminate information on lessons learned and best practices (by developing) dissemination strategies and tools such as websites, newsletters, etc." – *Department of Defense Year 2000 Management Plan, Version 2.1, September 1999, pg A-2*

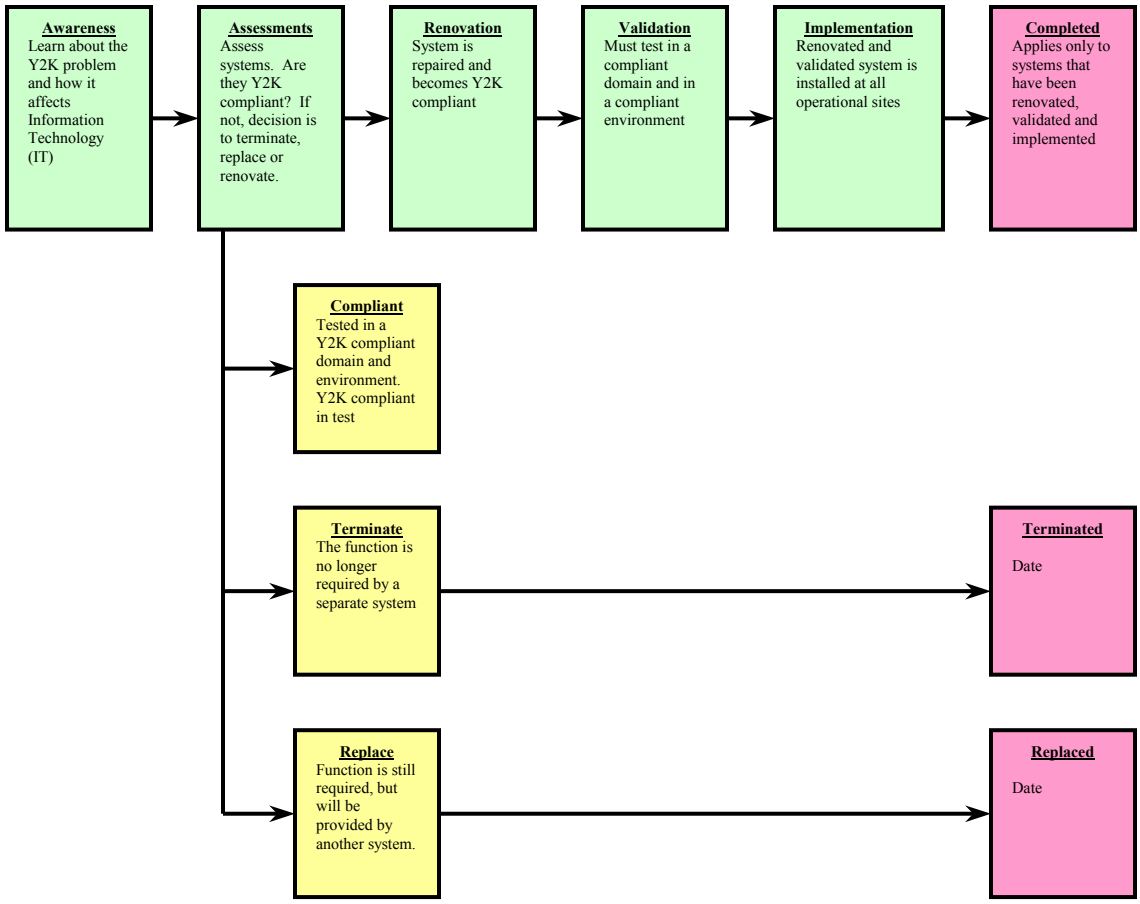


Figure 1: The DoD Year 2000 Five-Phase Management Process

The ***Assessment*** phase dealt with those activities required to define the size and scope of the problem, decide on the appropriate strategies to overcome it and establish a plan to put the necessary resources against the right tasks to ensure that systems were Y2K compliant. The primary deliverable of this phase was a project plan for each system (or group of systems that comprised a function or mission capability). The assessment was to start with a complete inventory of a Component's systems to get a handle on the scope of the total problem. The detailed assessment of each system was to include all hardware components, operating systems, database management systems (DBMS), software languages and compilers, system utilities, databases and files, and data interfaces and exchanges with other systems. Source code, vendor software and embedded chips were also recognized by the DoD as potential sources of Y2K compliancy problems.

Table 2: Exit Criteria for the Five-Phase Management Process

Phase	Minimum Exit Criteria
Awareness	• Component-level plan initialized • Y2K Points-of-Contact (POCs) identified and trained for all organizations • System users and owners identified and trained • Key DoD and industry Y2K POCs identified • Phase II (Assessment) strategy developed, documented and distributed • Managers at all levels aware of potential Y2K potential problems • Initiate inventory of systems to be replaced, renovated or decommissioned/retired
Assessment	• Phase II plan completed and distributed internally by the Component • Complete inventory of all systems and their external interfaces • Phase III (Renovation) strategy developed, documented and distributed internally by the Component • Identification of 100% of systems to be replaced, retired, renovated and certified as compliant • 100% of systems analyzed for Y2K compliance • Y2K procurement and resource strategy and plan developed and completed by each Component • 100% of systems requiring renovation prioritized and scheduled for Phase III • Risk management and contingency strategy developed and documented for each system
Renovation	• Phase III plan completed and distributed internally to each Component • Apply selected renovation strategy for all scheduled systems (strategy must be documented and communicated to interface partners) • Phase IV (Validation) strategy developed, documented and distributed by the Components • Phase V (Implementation) strategy initiated by the Component • Risk management and contingency strategy updated with dates for implementation of the contingency strategy
Validation	• Complete system testing • Complete system certification • Test and certify all interfaces • Updated contingency plan • Executive hardware/software used by an application must be compliant for certification • Waivers must be obtained for the continued use or procurement of any non-Y2K compliant hardware, software or firmware (including COTS/GOTS in mission-critical or mission-essential systems or applications) • Waivers also required for newly-developed mission-critical or mission-essential systems that are not Y2K compliant, or contain non-Y2K compliant COTS/GOTS
Implementation	• Risk management and contingency strategy updated and distributed • System successfully integrated and operational

The DoD recognized that there were many strategies available during the ***Renovation*** phase to make systems Y2K compliant (see Table 3), and emphasized the need for each Component to implement configuration management procedures to document all system changes. The intent was for DoD to take advantage of all Y2K-compliant Commercial Off-the-Shelf (COTS) or Government Off-the-Shelf (GOTS) solutions wherever practical to replace a system that exhibited Y2K problems, or to port an application to a modern

system architecture whose operating system and hardware had no Y2K issues, and to use software tools that help locate dates and related fields for Y2K "correction".

Table 3: Y2K Renovation Strategies

Renovation Strategy	Description
Accept	Determine that the date error will not impact the ability of the application to perform the Component's mission
Bridge	Utilize a bridge to convert date data received from other systems
Bridging	Converting data and coding to or from one type of conversion or "fix" to the "fix being applied in one system to another system"
Combination	Combine a number of various solutions which best meet the needs of the Component's mission and the interfaces
Conversion	Convert the date data, processing and interfaces to a 4-digit year format
	Consider changes in operating systems, compilers, utilities, domain-specific programming products, and commercial database management systems
Data Duplexing	Converting the two digit code into a four digit year replica
Date Field Compression	Compression of the two digit year field in a manner which will replace the two digit year code with a four digit year number at output
Date Field Expansion	Change the two digits to four-digit year fields in software and/or databases
Encapsulation	Shifting the year calculation or display downwards by 28 years
Fix	Fix the system by implementing a solution
Patch	Develop a patch code which will convert date data to a compliant, usable format
Replace	Replace the system; either migrate or a single system replacement
	Develop a new application, expand an existing application, or replace the functionality of a non-compliant system with commercial software
Retire	Retire the system – terminate
Terminate	Terminate the system or selected applications
Windowing	Use of a 100 year window (50 years for 1900s – 50 through 99, and 50 years for 2000s – 00 through 49) to convert data and code to the appropriate century)
Workaround	Develop a workaround for non-compliant systems
Wrapper	Implement a wrapper around a system or systems

Adapted from "Department of Defense Year 2000 Management Plan", September 1999, http://www.doncio.navy.mil/y2k/Y2KManagementPlan.pdf (Link active as of 6 February 2002), pp. A7-8.

The ***Validation*** phase of the Five-Phase Management Process dictated that operational tests must include mission support functionality. Prior to testing, a complete system

backup was required, including all operational software, system and application files, and mission-related data. It was also deemed necessary to completely isolate the system under test from all other systems to avoid leaking future dates into other systems and networks. The DoD Year 2000 Management Plan included numerous test cases that should be applied to test for Y2K compliance, based on routine tests that consisted of a set of exercises or system operations that would require the software to perform mission support functions exactly as they would in normal operation, as well as special test cases that were meant to focus on specific Y2K vulnerabilities beyond the "simple" rollover dates. These additional test cases targeted systems that calculated any sort of aging (e.g., 30 days past due, etc.), or addressed more general concerns (such as leap year testing for years 2000, 2001 and 2004). Table 4 represents the most crucial "future" dates identified in the DoD Year 2000 Plan (and other resources) that were to have been considered for Y2K compliance testing. It should be noted that there are several dates that have not yet rolled over and could represent potential problems for the DoD and its suppliers if not tested and certified beyond the basic rollover dates.

Table 4: Critical DoD Rollover Dates

Rollover Date	Significance
1995, Oct 01	Plans for 5 Fiscal Years or more extend to FY 2000
1996, Jan 01	Overflows Unisys mainframe 4-Year plans (budgets, op plans, strategies) end in 2000
1996, Oct 01	Plans for 4 Fiscal Years or more extend to FY 2000
1997, Jan 01	3-Year plans extend to 2000
1997, Nov 02	Overflow HP/Apollo Domain Operating System (OS)
1998, Jan 01	Ensure that the digits "98" do not trigger a red flag, result in erroneous branching, or otherwise cause a processing error or that "time error" faults occur. Also, to ensure that 31 December 1997 was calculated as the 365th day of 1997 (Found in Y2K patches in mainframes and elsewhere). 2-Year plans extend to 2000
1999, Jan 01	Ensure that the digits "99" do not trigger a red flag, result in erroneous branching, or otherwise cause a processing error or that "time error" faults occur. Also, to ensure that 31 December 1998 was calculated as the 365th day of 1998 (Found in Y2K patches in mainframes and elsewhere).
1999, Mar 01 **1999, July 01** **1999, Oct 01**	Check FY2000 for business and industry. Depending on the business, the FY could start on March 1st, July 1st, or match the Government fiscal year of October 1st.
1999, Aug 21	Global Positioning System (GPS) End-of-Week (EOW) Rollover Event #1
1999, Aug 21-22	Overflow of EOW rollovers (e.g., GPS rolls back to 1980-01-06; uses 1024-week cycle)
1999, Sept 09	Represents 9/9/99 or possibly 9999. Ensure that digits "99" or "9999" do not trigger a red flag, result in erroneous branching, or otherwise cause a processing error.
1999, Oct 01	First day of DoD Fiscal Year 2000
1999, Dec 31	End of file indicator for some old systems

Table 4: Critical DoD Rollover Dates (continued)

Rollover Date	Significance
2000, Jan 00	Ensure this date is **not** processed (some spreadsheets and database applications do have this problem and count January 0 as the day before the 1st)
2000, Jan 01	Key date in any compliance testing 1200 hours (noon). An embedded date chip failure has been found.
2000, Jan 03	First full work day in the new year
2000, Jan 04	For those organizations that had 03 January (Monday) as a holiday
2000, Jan 10	The first 7- or 8-character date in YYYY/M/DD or YYYY/MM/DD format (e.g., 2000/1/10 or 2000/01/10)
2000, Feb 28	Ensure that the leap year is being properly accounted for
2000, Feb 29	Ensure that the leap year is being properly accounted for
2000, Feb 30	Ensure that this date is **not** processed (found in some PC applications)
2000, Feb 31	Ensure that this date is **not** processed (found in some PC applications)
2000, Mar 01	Ensure that date calculations have taken leap year into account
2000, Oct 10	First 8-character string using a two-digit month (2000/10/10)
2000, Dec 31	The 366th day of the year
2001, Jan 01	The 1st day in the 21st century
2001, Feb 29	Ensure that this date is **not** processed as a leap year
2001, Sept 08	Ensure that the digits in 9/8/01 are not reduced to "99", thereby triggering a red flag or causing erroneous branching or other processing errors
2002, Jan 01	For any date on or past this day, ensure that no processing errors occur in backward calculations and processing of dates in the 1980s and 1990s at this point in time
2002, Feb 29	Ensure that this date is **not** processed as a leap year
2003, Feb 29	Ensure that this date is **not** processed as a leap year
2004, Jan 01	Simplex System date failure (used in security, access and fire systems)
2004, Feb 29	Ensure that this date **is** processed as a leap year
2004, Dec 31	The 366th day of the year and the 53rd week of the same year
2010, Jan 01	Overflow ANSI C Library
2019, Apr 06	GPS End-of-Week Rollover Event #2
2019, Dec 31	yy-date limit of Microsoft Excel 95
2024, Unk	Overflow problem with older Unix and other systems. Precise date and cause were still being researched as of September 1999
2029, Dec 31	yy-date limit of Microsoft Excel (next major version)
2030, Unk	A breakpoint in Microsoft (MS) windowing system, i.e., the years 2029 and 2030 will imply the year 1930
2034, Jan 01	Share/43 rolls back to 1970
2034, Sept 30	Overflow of Unix time function
2036, Dec 31	Date limit of Visual C++ (4.x) runtime library
2037, Jan 01	Rollover date for NTP systems
2038, Jan 19	Overflow of Unix systems, C and C++
2038, Nov 20	GPS End-of-Week Rollover Event #3
2042, Sept 18	Overflow of IBM System/360
2049, Dec 31	Date limit of Microsoft Project 95 and previous versions
2058, July 06	GPS End-of-Week Rollover Event #4
2072, Unk	Overflow of Milstar Operating System
2078, Feb 19	GPS End-of-Week Rollover Event #5
2097, Oct 05	GPS End-of-Week Rollover Event #6
2100, Feb 28	Last day of February, **not** a leap year
2101, Mar 01	"Terminal" date, used to encompass all established rules for calculation of dates and calendar events

Once the Y2K system had been renovated, validated and certified as compliant, it could enter the ***Implementation*** phase. The DoD plans called for implementation scheduling that would deal with the uncertainties common to all large system development efforts. The schedules were to indicate all major milestones, and identify the critical path(s), for the completion of the Y2K program. Implementation concerns that were to be planned for and dealt with needed to be resolved prior to implementation in order to ensure that:

- all outside data exchange entities were notified
- data bridges and filters were capable of handling non-conforming data
- contingency plans, which had been developed during the Assessment phase of the process, were updated and in place in case invalid data were received from an external source
- a process was in place for validating incoming external data prior to running any live applications

The test model was built upon and complemented the Five-Phase Management Process. The five levels of test activity spanned all five phases of the management model, with the majority of the testing scheduled to take place during the renovation and validation phases. Table 5 illustrates the concepts associated with each of the five test phases.

Table 5: Y2K Test Model Elements

Element	Actions
Testing Infrastructure	• Assign Y2K test management authority and responsibility • Define compliance criteria • Develop test and evaluation master plan (TEMP) • Define and secure test resources • Establish test environment • Develop and issue test guidance • Establish processes and information sources to support testers • Ensure Year 2000 compliance of vendor-supported products and services • Establish processes and metrics for test reporting • Establish test tools
Software Unit Testing	• Schedule and plan software unit test • Prepare test procedures and data • Define test exit criteria • Execute tests • Document test results • Correct defects • Ensure that test exit criteria satisfied

Table 5: Y2K Test Model Elements (continued)

Element	Actions
Software Integration Testing	• Schedule and plan software integration test • Prepare test procedures and data • Define test exit criteria • Execute tests • Document test results • Correct defects • Ensure test exit criteria satisfied
System Acceptance Testing	• Schedule and plan system acceptance test • Prepare test procedures and data • Define test exit criteria • Confirm Y2K compliance of vendor-supported system components • Execute tests • Document test results • Correct defects • Ensure test exit criteria satisfied
End-to-End Testing	• Define end-to-end test boundaries • Secure data exchange partners' commitment • Establish end-to-end test team • Confirm Y2K compliance of vendor-supported telecommunications infrastructure • Schedule and plan end-to-end tests • Prepare test procedures and data • Define test exit criteria • Execute tests • Document test results • Correct defects • Ensure test exit criteria satisfied
Management and Oversight Control	• Ensure that established test activity and progress reporting requirements are met • Solicit reports from the Quality Assurance/IV&V and user groups • Identify and assess deviations from plans • Take appropriate action to address deviations

3.2 Contingency Planning and Risk Management

To ensure continuity of operations, contingency plans were to be developed. These plans were to address (1) known or suspected sources of disruption, and (2) unanticipated disruptions. Contingency plans were to address failure of systems believed to be Y2K compliant, transfers of corrupt data between systems, failures of utilities or infrastructure elements necessary for operation, or any other items that could result in a Y2K-related failure. They were to include "back to basics" approaches that could be used to sustain mission-critical capabilities. All plans needed to be tested to ensure their effectiveness.

The DoD identified Operational (Mission/Functional) and System (Technical) Contingency Plans as being necessary to capture the most critical aspects of Y2K

contingency planning. Each type of plan was to be the responsibility of a different management level and have a different focus. The Operational Contingency Plan would focus on the completion of a stated mission or function without the support of any or all of the mission-critical support systems. The System Contingency Plan would focus on the basic restoration of a system. Appendix H of the Department of Defense Year 2000 Management Plan, Version 2.1, September 1999 (http://www.doncio.navy.mil/y2k/Y2KManagementPlan.pdf) contains more detailed information on these two types of CPs. The level of detail within these plans was expected to be system-dependent on complexity and mission criticality. Previous versions of the aforementioned Management Plan had also discussed Programmatic CPs, which were part of the Assessment phase and the Risk Management process for system renovation. All Programmatic CPs were expected to have been completed by the September 1999 date of Version 2.1 of the Management Plan.

Although the OASD(C3I) Office did not intend to collect and review all contingency plans, the Components were expected to review them (and those of their subordinate commands) to the necessary level of detail to ensure that all operational objectives were met or mitigated.

Risk management was to be applied to the Y2K correction process to identify system-related risks, and how the system might fail, before they could adversely impact execution of the mission. Failures could include something that stopped working, something that worked but did not reflect correct dates, or something that appeared to work but passed incorrect data to interfacing systems. Risk assessment was to be used to determine how the failure of a system would affect the mission it was intended to support. Eliminating these risks could include renovating or replacing a system, devising workarounds, or a combination of these actions. Mission-critical systems received the highest priority in both risk management and contingency planning.

It was expected that employing risk management would ensure that:

- All Y2K issues would be identified

- Fixes for all Y2K issues would be identified
- A feasible schedule of fixing and testing the system or device would be followed
- Resources (personnel, funding, facilities, etc.) would be available and dedicated to accomplish the fixes
- System testing would be fully planned and scheduled
- All interfaces would be identified and tested, and all Interface Agreements would be in place
- The fix and test schedule would include adequate time for unforeseen problems
- A test site with Y2K-compliant software would be available
- The system or device would be fully operational during the Implementation phase.

DoD Components were also responsible for developing a Component Continuity of Operations Plan (COOP). The plan was to include a prioritized list of Component systems and the major actions taken to minimize Y2K disruption. The list was to be used to prioritize the response sequence and resource use in the event of widespread disruptions. For example, ASC(C3I) disseminated the "DoD Y2K Management Plan" guidance on continuity of operations and contingency planning. The office tracked and summarized the status of all systems affected by Y2K.

3.3 The DoD Y2K Database

The DoD Defense Integrated Support Tools (DIST) database was established to provide a composite picture of DoD Y2K information and serve as the centralized repository of Y2K management data for the DoD. Information on each system, their programs, platforms, and languages was to be tracked in the DIST. The database was to be used to meet forecast reporting requirements that were levied on the DoD by the Office of Management and Budget (OMB) and others. It would provide a summary level Y2K

management and analysis tool within and for DoD, and serve as the single official source for reporting the status of systems to senior management and the OMB.

Table 6 provides a summary of the concepts that drove the DoD Y2K Database characteristics. Table 7 provides an overview of the responsibilities borne by OSD as the maintainer of the database.

Table 6: Concepts That Drove the DoD Y2K Database

• Minimize all duplicate reporting requirements levied on the Agencies and Services
• Maintain accurate and current data to track "enterprise-wide" DoD Y2K status at OSD
• Minimize the impact to Agencies and Services of reporting requirements from OMB and the General Accounting Office (GAO)
• Provide established, defined reports that are easily accessible to appropriate offices
• Allow the intelligence community to maintain a separate, but similar, database to maintain the integrity of their data and independently report to Congress and OMB. Provide a regular declassified abstract of status records for loading into the standard Y2K database to allow roll-up reporting for all of DoD.
• Provide data and structure for supporting future OSD analysis requirements regarding Y2K readiness
• Create a means to provide an automated OMB report and real time interactive reporting to the Y2K Steering Committee meetings
• Provide a single source for the current status of mission-critical and mission-essential systems throughout the entire DoD

Table 7: OSD Responsibilities for Maintaining the DoD Y2K Database

• Coordinate with the appointed Points of Contact for each Component
• Aggregate the Component data in the database from the files provided by each Agency and Service Component
• Maintain the DoD database software/hardware upgrades and releases
• Establish schedules for data submission
• Provide for configuration management
• Provide Help Desk support
• Provide ad hoc reporting

3.4 Reporting

The reporting aspects of the DoD DIST database and process were established to meet the Y2K reporting requirements levied by Congress, the OMB, and the DoD. The process was designed to accomplish Y2K reporting requirements without imposing additional data calls on the DoD Components. Components maintained ownership of

their data and provided periodic reports to OSD. The OMB actually had two separate requirements for Y2K status reporting. The first was a Quarterly Report to OMB, required of all Federal agencies. The second was a monthly report required for all "Tier One" Federal agencies that were judged to be making insufficient progress toward Y2K compliance. The focus of these reports was very different, as illustrated in Table 8.

Table 8: Focus of OMB Y2K Reports

Report Type	Report Focus
Monthly Report	• Monthly reports included all statistics and charts • Focus was on a comparison of projected and actual progress in each stage of remediation • The OMB Monthly Report Requirements were detailed in a series of Memorandums (e.g., M-99-21, "Revised Reporting Guidance on Year 2000 Efforts", dated 06 Aug 1999 and M-99-09, "Revised Reporting Guidance on Year 2000 Efforts", dated 26 Jan 1999) • The data for the OMB Monthly Reports were to be taken directly from the DoD Y2K database • The data were to be pulled from this database on the first of each month for the report due to OMB on the 10th of each month
Quarterly Report	• Quarterly reports were intended to be much more comprehensive, requiring information on interfaces, systems behind schedule, systems scheduled for completion after milestones, estimated costs, and information on embedded systems • Provided a forum for OMB to collect information on special interest items, and for Agencies to discuss new initiatives • The OMB Quarterly Report Requirements were also detailed in a series of Memorandums (e.g., M-99-21, "Revised Reporting Guidance on Year 2000 Efforts", dated 06 Aug 1999 and M-99-09, "Revised Reporting Guidance on Year 2000 Efforts", dated 26 Jan 1999) • The data required for the OMB Quarterly Report were defined in Appendix L of the DoD Year 2000 Management Plan • The information in this report was to have been submitted to OSD by each Component and Agency, both electronically and by signed copy, on the 15th of January, April, July and October

The goal of the OMB Y2K reporting requirements was to provide consistent, timely and accurate reporting. As a result, DoD was directed to extract all reasonable and prudent

data from the OSD Y2K database. Once the DoD Y2K database had all data elements activated and fully populated, only new and special interest items would require an additional data call.

4 The Implementation

In November 1995, the Chief Information Officer of the DoD issued an "All Hands" message which launched the Awareness phase of the DoD five phase management process. Subsequent instructions from Departmental leaders, including the Deputy Secretary of Defense, increased awareness at all levels in the Department. Memoranda and guidance followed from senior leaders in the Military Departments, Defense Agencies, and Joint Staff Components.

Recognizing that the Year 2000 problem needed to be addressed in both the DoD's software and hardware systems, an additional memorandum was issued in May 1996 regarding the problem in personal computer (PC) and workstation Basic Input Output System (BIOS) chips. The memorandum directed DoD managers to have prime contractors for PCs, workstations, and software certify that their products were Y2K compliant. Stop Work orders were issued to those contractors that failed to comply.

4.1 DoD Organization

Much of 1998 was spent getting a management structure in place to focus the DoD efforts on Y2K so that the management strategy could be effectively implemented. Y2K efforts in the DoD were organized to ensure enterprise-wide leadership. The roles and responsibilities defined for organizations and individuals within the DoD to address the Year 2000 problem are summarized in Table 9. All of these roles and responsibilities were assigned within the context of existing laws, Executive Orders, DoD Directives and Instructions, and other approved DoD policies.

Table 9: Key DoD Roles and Responsibilities to Address Y2K

DoD Organization	Roles and Responsibilities
Deputy Secretary of Defense (DepSecDef)	• Chaired the DoD Y2K Steering Committee
Principal Staff Assistants (PSAs)	• Provided functional end-to-end test plans to DepSecDef • Certified that test plans included assessments of functional risk, effects of Y2K on continuity of business operations, and associated contingency plans • Ensured that all test plans included a listing of all mission-critical systems involved in the test • Coordinated each test plan with the Military Departments and all other pertinent PSAs
DoD Chief Information Officer (CIO)	• Formulated, implemented and was responsible for the DoD Y2K program • Represented DoD on the President's Council on Year 2000 Conversion, and coordinated the DoD efforts to support the Council • Established and maintained DoD-wide policy guidance and strategies addressing the Y2K problem • Served as the Executive Secretary to the DoD Year 2000 Steering Committee • Served as Chairman of the High Risk Systems Boards
DoD Deputy Chief Information Officer	• Served as the focal point for coordinating DoD-level Y2K policies, strategies and initiatives • Served as the focal point for consolidation and coordination of all DoD-wide Y2K reporting requirements from the Congress, the Office of Management and Budget (OMB), the Federal CIO Council, and other Federal organizations as required by the DoD CIO • Developed initiatives to increase Y2K awareness and improve readiness • Established Y2K reporting requirements in accordance with Congressional and OMB guidance, and maintained the DoD Y2K reporting database • Monitored progress to ensure that DoD objectives were met • Developed a certification process for Y2K compliance • Chaired the DoD Y2K Working Group, as described in the Y2K Steering Committee Charter • Approved/disapproved waivers for the procurement or continued use of non-Y2K compliant products that were expected to be used in mission-critical or mission-essential applications beyond the Y2K rollover dates • Coordinated the representation of DoD in Y2K discussions, working groups and meetings with other Government branches and organizations, including the President's Council on Y2K Conversion • Established a Classified Programs Monitoring Team that ensured that all classified system Y2K information was reported and evaluated • Provided support activities to the DoD CIO for the DoD Y2K Steering Committee • Provided advisory support to all DoD organizations in policy, budgetary and legislative matters related to Y2K • Served as the Co-Chair with Joint Staff for all Y2K Readiness Reviews
Deputy Assistant Secretary of Defense for Intelligence and Security – OASD(C3I)	• Coordinated efforts to address Y2K issues throughout the DoD Intelligence Community

Table 9: Key DoD Roles and Responsibilities to Address Y2K (continued)

DoD Organization	Roles and Responsibilities
DoD Components	• Established and maintained Component-wide Y2K Management Plans and Contingency Plans appropriate for their missions and functions • Planned for and executed corrective actions to ensure Component-wide Y2K compliance • Conducted system level tests to validate compliance of systems that had been repaired (i.e., "renovated"), and participated in function- and mission-level testing that included domain testing by DISA megacenters, as well as exercises by the CINCs • Established a Component-wide Y2K Program Office with oversight responsibility • Provided accurate and timely input of all required data to the DoD Y2K database and other reporting requirements that were directed by OSD • Established a means of tracking the status of Y2K efforts that included performance metrics for all Component systems • Provided a Component Y2K representative to participate in the DoD Y2K Workgroup and other DoD Y2K collaborative bodies as requested by OSD • Employed Service and Agency IG/Auditors to monitor Y2K progress
Director, Defense Information Systems Agency (DISA)	• Maintained a current and accurate listing of all tools available to assist in resolving Y2K problems, and of all commercial and Government off-the-shelf (COTS/GOTS) products (i.e., operating systems, database management systems (DBMS), hardware, BIOS chips, etc.) • Provided technical assistance to the Components • Functioned as the Y2K Testing Information Clearinghouse for DoD • Reported to the DoD CIO on the status of specific and explicit test agreements between domain users and DISA megacenters
Individual Program/Project/Product Managers (PMs)	• Purchased only Y2K compliant products • Included Y2K compliance language in all new contracts and contract modifications, as appropriate • Documented systems interfaces and obtained Interface Agreements, or the equivalent, for each system interface • Certified or retired each system, as appropriate • Developed and maintained all necessary documentation that supported certification of Y2K compliance • Developed and maintained system contingency plans

The DoD Y2K Steering Committee, which was chaired by the Deputy Secretary of Defense (DepSecDef), was established to oversee progress, provide guidance and make decisions related to Y2K. The committee also served as a forum to facilitate the sharing of information, eliminate overlapping tasks/responsibilities, and identify cross-functional issues or opportunities that would accelerate the identification and implementation of Y2K system fixes. Membership on this committee included the DoD Chief Information Officer (CIO), OSD Principle Staff Assistants (PSAs), senior military leaders from each

of the Services, and additional members, as requested by the DepSecDef. In addition, the Chairman of the President's Council on Y2K Conversion also participated in the DoD Y2K Steering Committee meetings.

The Principle Staff Assistants (PSAs) of the Office of the Secretary of Defense (OSD) were responsible for verifying that all of the functions over which they exercised control would not be adversely affected by Y2K issues. The specific PSAs included:

- Under Secretary of Defense(Acquisition and Technology) – USD(A&T)
- Under Secretary of Defense (Policy) – USD(P)
- Under Secretary of Defense (Personnel and Readiness) – USD(P&R)
- Under Secretary of Defense (Comptroller) – USD(C)
- Assistant Secretary of Defense (Command, Control, Communications and Intelligence) – ASD(C3I)

The DoD Chief Information Officer (CIO) and his Deputy were responsible for overseeing the Department's correction of the Y2K problem.

The Deputy Assistant Secretary of Defense for Intelligence and Security, OASD(C3I), had the overall responsibility for coordination of Y2K efforts to address all issues throughout the DoD Intelligence Community.

The DoD Components were responsible for the implementation, execution, testing and performance of Y2K efforts within their respective Components. For each and every system for which a DoD Component was responsible for development or maintenance, the Component:

- inventoried all systems and identified each system as being either mission-critical or non-mission-critical
- assessed and implemented an appropriate strategy to make each system Y2K compliant

- prioritized each system according to the Component's Y2K strategy
- informed other DoD Components and/or CINCs that were dependent on the system as to the status of the Y2K efforts affecting that system so that appropriate mitigation plans could be developed
- identified, prioritized and mobilized personnel resources, as needed, to address and solve Y2K problems
- reallocated and reprogrammed Component-wide resources to support all Y2K efforts
- identified budget shortfalls and included them in all budget submissions and reprogramming actions
- defined Y2K responsibilities for their Program and System Managers
- implemented the use of Y2K compliance language as provided in the Federal Acquisition Regulations (FAR) 48 CFR, Parts 39.002 and 39.106, which addressed Y2K compliance definitions and language
- issued "Stop Work" orders on all existing contracts for products that failed to meet Y2K requirements, or requested a waiver from the DoD CIO

The DoD Y2K Working Group supported all of the activities and deliberations of the DoD Y2K Steering Committee, investigated Y2K issues, provided recommendations, and identified and shared corrective actions and lessons learned. This group was chaired by the Deputy CIO.

4.2 DoD Actions, Activities and Implementation

The DoD recognized that the first line of defense against the combination of inherent vulnerabilities and increasingly sophisticated multi-faceted threats against the Defense Information Infrastructure (DII) throughout the Y2K rollover and beyond would be the DoD system users, administrators and managers. The DoD established Computer Emergency/Incident Response Teams and Vulnerability Assessment Teams that were to be notified in the event of any suspicious activity occurring within DoD systems and/or networks, regardless of whether it originated from an insider or external source. These teams were also used to examine and assess systems after Y2K renovation and validation.

Table 10 identifies the key Computer Emergency Response Teams (CERTs) that were active during the Y2K effort. (*These teams continue to have active Web pages as of mid-March 2002 and are serving as a resource for reporting and coordinating activity relative to potential threats to DoD information systems and critical infrastructure*). Internet links to these CERTs are also provided in the table.

Table 10: Computer Emergency Response Team Resources

CERT	Description	Internet Link
CERT/CC	• Computer Emergency Response Team Coordination Center • Formed by the Defense Advanced Research Projects Agency (DARPA) in 1988 in response to needs identified during an Internet security incident • Chartered to work with the Internet community in detecting/resolving computer security incidents, as well as taking steps to prevent future incidents • Provides incident reporting and incident recovery support services	http://www.cert.org/
ACERT	• Army Computer Engineering Response Team • Conducts Command and Control Protect (C2P) operations in support of the Army • Ensures the availability, integrity and confidentiality of the information and information systems used in planning, directing, coordinating and controlling forces in the accomplishment of Army missions across the full spectrum of military operations • Link may no longer be active as of 15 February 2002	http://www.acert.belvoir.army.mil/
NAVCIRT	• Naval Computer Incident Response Team • The Navy's single point of contact for reporting and handling computer security incidents and vulnerabilities	http://infosec.nosc.mil/
AFCERT	• Air Force Computer Emergency Response Team • Established by the Air Force Information Warfare Center (AFIWC) as the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities reported by AF computer users, security managers, system managers and Air Force Network Control Centers (AFNCC) • Coordinates the technical resources of AFIWC to assess, analyze and provide countermeasures • Link may no longer be active as of 15 February 2002	http://afcert.csap.af.mil/
DISA	• Defense Information Systems Agency • The DoD principle agent for the management of the Defense Information Infrastructure (DII) • Operates an Automated Systems Security Incident Support Team (ASSIST) to identify, analyze, assess and resolve DII Information Assurance Vulnerabilities, anomalous activities and penetrations	ftp://ftp.assist.mil/ (****.mil sites only!)***

The DoD adopted standard compliance language that was published in the Federal Acquisitions Circular and added to the Defense Acquisition Deskbook. This standard

acquisition language helped to ensure Year 2000 compliance in DoD purchases of both software and hardware.

The Military Departments and Agencies each prepared individual management plans for Year 2000 Information Technology compliance. Each plan described the approach for determining priorities of fixes, contingency plans, and status of implementation schedules.

The Y2K Interface Assessment Workshops (IAWs), which were started during August 1996, addressed the interface issues and operability concerns that were associated with the 21 different functional areas that the DoD needed to address to ensure that the DoD's end-to-end functionality was not impaired by the Y2K problem. A joint memorandum to the Defense Agencies and Military Departments was signed by the Under Secretary of Defense (Comptroller) and the Office of the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence (OASD(C3I)). It required registration in the DIST of information systems, system interfaces, and data exchanges. Systems that were not registered in DIST ran the risk of loss of funding. Each Workshop was intended to focus on one or more functional areas. The DoD CIO (or designated representative) and a specific OSD-level functional area proponent co-chaired each Workshop, which was coordinated with the assistance of the Components' representatives to the Y2K Working Group.

Y2K Readiness Reviews were structured to review progress toward demonstrating an increasing level of confidence that the Department would be able to execute its warfighting operations and support functions after the Y2K rollover. The reviews provided a framework for inter-service, inter-agency, inter-department and cross-functional coordination to synchronize their efforts. Each review brought together OSD, Joint Staff, Service, Agency, Principle Staff Assistant and appropriate non-DoD representatives. The reviews were co-chaired by the Joint Staff and OSD, and provided a forum to ensure commonality of approach and consistent interpretation of relevant laws and mandates. The format of these reviews also ensured the optimum use of DoD

resources while providing effective coverage of critical operations. This ultimately facilitated the overall risk management process and subsequent resolution of conflicts and schedules.

4.3 Pre-Rollover Status of Y2K Efforts

Beginning in July 1996, and continuing throughout the entire Y2K process, the Subcommittee on Government Management, Information and Technology periodically prepared and issued a "Report Card: Year 2000 Progress for Federal Departments and Agencies" as a means of providing insight into progress being made, as well as holding the departments and agencies accountable for their progress (or lack thereof) in meeting the Y2K program objectives. Table 11 shows how the Federal Government fared just prior to the rollover event using the final Y2K Report Card (November 1999) as an example. All grades were based on mission-critical systems only, as well as associated criteria that included percentage of compliant systems, existence of contingency plans, coverage of telecommunications systems, coverage of embedded systems, external data exchange capabilities, and status of verification efforts. The information in Table 11 is grouped according to letter grade as of November 1999 (the right-most column).

Table 11: The Year 2000 Report Card (22 November 1999)

	96 July	**98** May	**98** Aug	**98** Nov	**99** Feb	**99** June	**99** Aug	**99** Nov
SSA Social Security Administration	A	A+	A	A	A	A	A	**A**
NRC Nuclear Regulatory Commission	B	B	D	C-	A	A	A	**A**
FEMA Federal Emergency Management Agency	F	A-	B-	B	B+	A	A	**A**
HUD Dept. of Housing and Urban Development	D	C	C	C	A-	A	A	**A**
Education Dept. of Education	B	D	F	C-	A-	A	A	**A**
NSF National Science Foundation	C	A-	A	A	A	A	A	**A**
GSA General Services Administration	D	C-	D	B	A-	A	A	**A**
Labor Dept. of Labor	F	C	D	C	B	A	A	**A**
VA Dept. of Veteran Affairs	D	C	B-	B-	A-	A	A-	**A**

Table 11: The Year 2000 Report Card (22 November 1999) (continued)

	96 July	98 May	98 Aug	98 Nov	99 Feb	99 June	99 Aug	99 Nov
Interior Dept. of the Interior	D	C-	D	B	A-	A-	A-	**A**
NASA National Aeronautics and Space Admin.	D	B	C+	C+	B+	B	B+	**A**
DOE Dept. of Energy	F	F	F	F	B	C+	B	**A**
OPM Office of Personnel Management	A	C-	D	C-	A-	A	A	**A-**
Commerce Dept. of Commerce	D	B	B	B	B	B	B	**A-**
Agriculture Dept. of Agriculture	D	D	C	C	C	C+	C-	**A-**
SBA Small Business Administration	A	B	A	A	A	A-	A-	**B**
State Dept. of State	B	F	F	F	F	A-	A	**B**
DOT Dept. of Transportation	F	F	D	D	F	C	B-	**B**
AID Agency for International Development	A	F	F	F	F	F	D	**B**
EPA Environmental Protection Agency	D	F	B	B+	A	A	A-	**B-**
DoD Dept. of Defense	C	D	D	D-	C-	C-	D	**C+**
HHS Dept. of Health and Human Services	D	F	F	F	C+	B-	C	**C**
Treasury Dept. of the Treasury	C	C	D+	C	B-	C	C-	**C**
Justice Dept. of Justice	D	D	F	F	B	C	C-	**D**
Administration Overall Federal Departments and Agencies	*	F	D	D	C+	B-	B-	**B+**

*Administration grade not given

Some of the reasons for the low DoD grades were due to a perceived lack of strong management and oversight controls over the Year 2000 mediation efforts. The report "Defense Computers: Year 2000 Computer Problems Threaten DoD Operations" (GAO/AIMD-98-72), issued in April 1998, highlighted the steps that DoD had failed to address that were fundamental to correcting mission-critical systems on time. These included:

- DoD did not yet have a complete inventory of systems, so that it could not reliably determine what resources it needed or identify problems requiring greater management attention

- DoD had not ensured that mission-critical systems were receiving a higher priority than non-mission-critical systems

- DoD had not identified all systems interfaces, nor ensured that its Components were effectively working with their interface partners to correct the interfaces

- DoD had not ensured that facilities were available for Year 2000-related testing, or that Component testing requirements were consistent

- DoD did not know if Components had developed contingency plans necessary to ensure that essential mission functions could be performed even if critical mission systems were not corrected in time

- DoD did not have a reliable estimate of Year 2000 problem correction costs

From April 1998 through November 1999, DoD was apparently able to make progress in addressing these weaknesses, but only enough to raise their November 1999 grade to a C+, so that there was only a slightly better than average perception that DoD would survive the rollover without some significant problems.

As a summary of its activity over the course of the Y2K preparation effort leading up to the rollover, the DoD:

- identified 2,367 mission-critical systems and 5,488 support systems at 637 military sites worldwide (as of 15 November 1999)

- identified 4,221,565 embedded devices that needed to be addressed

- conducted 123 major evaluations (including 36 by the Unified Military Commands)

- performed 180 audits for Y2K compliance

Costs for the Department's Y2K program totaled $3.596 billion over the six-year period, Fiscal Years 1996-2001. This price tag covered such factors as identifying the problem, fixing systems, conducting tests, developing contingency plans, and running extensive operational evaluations.

The Department's final completion rate was put at 99.9 percent. Two mission-critical intelligence systems would not be finalized until May 2000. The DoD Inspector General that monitored the Department's progress stated that "the cumulative results of the extensive audit and inspection effort to facilitate and validate DoD Year 2000 conversion progress support an assessment that the Department is ready to carry out all national security missions after December 31, 1999."

5 The Rollover

As the Year 2000 rollover began on 31 December 1999, Y2K had little or nothing to show for itself at DoD bases in Europe and the Middle East as far as widespread computer failures or coordinated acts of cyber-terrorism were concerned. All systems remained operational throughout Europe, and DoD did not receive any calls for assistance from foreign governments or U.S. embassies abroad. While crowds gathered in major cities throughout Europe and the Middle East in defiance of potential electronic infrastructure meltdown, the U.S. Air Force greeted the rollover with the first DoD baby and "a quiet evening with no significant incidents."

On 1 January 2000, the Deputy Defense Secretary reported that operations were "absolutely normal". While most of the rollover period was uneventful, one significant problem was encountered. A satellite-based intelligence system experienced a Y2K failure shortly after the rollover to Greenwich Mean Time. During the outage, intelligence officials could not process information from the system for three hours. "The problem wasn't with the satellite system — they were under positive control at all times," the Deputy Defense Secretary stated. DoD officials were able to go to a contingency plan and were able to restart processing information from the satellite before midnight Washington time. The Defense Secretary noted that "all of our high priority needs, for the DoD and other national customers, are fully being met." There was little evidence of hacking into DoD computers during the rollover.

The enormous efforts that DoD undertook to ensure Y2K readiness were largely successful. As an example, only 61 out of 1,059 logistics systems experienced notable failures during or following 1 January 2000. Of the 61 systems with failures, 60 were non-mission-critical systems that were not exposed to end-to-end testing. Technicians were able to correct the Y2K problem for the one mission-critical system (Streamlined Automated Logistics Transmission System) within hours of the failure based on their experience with a nearly identical problem during Y2K testing.

In general, there were few significant Y2K failures reported internationally, and none that immediately impacted the safety of American citizens worldwide. The global success was attributed, in large part, to the U.S. Government's international outreach and awareness campaign led by the Department of State, the Department of Defense, and the President's Council on the Year 2000 conversion, in coordination with the United Nations and World Bank. Appendix A includes a comprehensive list of international incidents that occurred as part of the Y2K rollover. The following list provides a very small sampling of confirmed Y2K failures that indicate what might have happened had the problem not been addressed:

Canada:	Computer controls on prison cell doors failed
Kazakhstan:	Ekibastuz Hydroelectric Power Station-2, as of 27 January 2000, had been handling its technology processes manually since 1 January 2000 due to non-compliant computers
Spain:	Y2K problems were experienced in control systems for 2 out of 9 nuclear reactors
United States:	The Federal Reserve Bank in Chicago reported a Y2K glitch in transferring about $700K in tax payments from customers of 60 financial institutions in the region
Zimbabwe:	The City of Harare's financial system failed

At the first meeting of the Network Reliability and Interoperability Council (NRIC) V, in August 2000, Ms. P.J. Aduskevicz of AT&T congratulated the industry and the NRIC on its successful Y2K and Leap Year transition, attributing this high level of success to:

- Many potential problems being fixed in advance
- Many potential problems having been exaggerated

- ***Many potentially faulty systems having been turned off (emphasis added)***
- Some systems having lower load and others having higher degrees of support than anticipated or normal
- ***Some problems were de-emphasized, ignored, or not reported (emphasis added)***
- Some problems occurred in the Third World where there was less dependency on computer technology

6 Lessons Learned

Prior to the Y2K rollover, a significant number of lessons learned, both positive and negative, were already identified as being significant for the continued improvement in the management and implementation of Information Technology.

The U.S. Senate Report, "Investigating the Year 2000 Problem: The 100 Day Report", published on 22 September 1999 looked at the preliminary "big picture" to categorize two lessons learned:

- The Y2K problem caused organizations worldwide to re-examine their use of information technology and, in some cases, to streamline operations (i.e., "a more efficient use of technology can lead to continued economic growth")
- Y2K greatly heightened awareness of the vulnerabilities that the extensive and interconnected use of technology creates in our critical infrastructures, i.e., those computerized and physical services that are essential to the basic functioning of the economy and the Government

In a 27 December 1999 article, the Technical Director for InfoWorld Test Center and acting Section Editor for Enterprise Computing, Maggie Biggs, identified 10 lessons learned that companies could take away from the Y2K experience. This list, published in the fashion of David Letterman's "Top Ten" list, is presented below:

10. **Technology Dependency:** IT needs to account for the organization's issues and concerns, as well as identify dependencies and needs of those outside the company.

9. **Out with the Old, In with the New:** Examining Y2K costs vs. future strategic planning should force a re-evaluation of the financial rationale for maintaining systems for an extended period. The outside boundary should be shortened to avoid excessive costs for vendor and IT support.

8. **Complex Coping Strategies:** The Y2K software bug was technically simple, but had tremendous business impact. The Y2K experience baseline should be used for defining future coping strategies for complex issues.

7. **Software Quality:** Companies that are building applications should draw on the lessons learned during Y2K to formulate a set of corporate development standards that ensure high quality.

6. **Business Recovery:** Y2K contingency plans could easily be updated to an overall business-recovery plan. Y2K should show that organizations can, and should, regularly update contingency plans.

5. **Inventory Management:** The inventory information identified during Y2K can be re-used to update an organization's asset information, and to update or create an applications catalog.

4. **Project Management and Problem Solving:** Leaders on Y2K projects know that solid project management and good problem-solving capabilities were required. Applying the same level of attention to future projects will help to increase project success rates.

3. **Documentation:** The perspective needs to be adopted that proper documentation is truly important, and its priority needs to be increased in the project plan.

2. **Technical Resources:** The Y2K effort required significant technical staffing. Beyond the rollover, many of these people will be seeking opportunities. Retraining will be needed to move them into other areas, but the investment will pay off over the long term.

1. **Business and IT Partnerships:** Y2K projects increased communications between the business and technology areas within many organizations, and new partnerships were formed. These alliances should continue to be leveraged for future projects (e.g., e-business).

Bonus: Think carefully about all design and implementation strategies so that an immense problem is not created for the next generation of IT troubleshooters.

Some of the key partnerships that evolved over the Y2K effort are highlighted in Table 12, identified by industry sector, the participating trade association, and the lead Federal organization. Also included is an overview of how the National Y2K Information Coordination Center (ICC) overlaid its efforts into key private sectors.

Table 12: Key Y2K Private/Public Partnerships and ICC Structure

Sector	Trade Association	Lead Federal Organization
Airlines	Air Transport Association	Department of Transportation
Cyber-Assurance	Cyber Assurance National Information Center	Information Coordination Center
Electric Power	North American Electric Reliability	Department of Energy
Financial Services	Securities Industry Association	Securities and Exchange Commission
Natural Gas	American Gas Association Interstate Natural Gas Association of America	Department of Energy
Oil	American Petroleum Institute	Department of Energy
Pharmaceuticals	National Pharmaceutical Alliance National Association of Chain Drug Stores	Department of Health and Human Services
Retail	National Retail Federation	Information Coordination Center
Telecommunications	Network Reliability and Interoperability Council	National Communications System

Sector	Lead Federal Organization(s)
Building Operations	General Services Administration
Chemical-Related Manufacturing	Environmental Protection Agency
Communications	Federal Communications Commission (FCC) General Services Administration
Cyber-Assurance	Information Coordination Center (ICC) Critical Infrastructure Assurance Office Federal Computer Incident Response Capability National Infrastructure Protection Center
Drinking Water	Environmental Protection Agency
Education	Department of Education
Emergency Services	FEMA
Employment-Related Protection	Department of Labor
Energy	Department of Energy
Federal Benefits Payment Programs	Social Security Administration
Financial Services	Federal Reserve Board
Food Supply	Department of Agriculture
Hazardous Materials	Environmental Protection Agency U.S. Coast Guard
Health Care	Department of Health and Human Services
High-Impact Federal Programs	Office of Management and Budget
Mission-Critical Systems	Office of Management and Budget
National Security & International Affairs	Department of Commerce Department of Defense Department of State
Public Safety	Department of Justice
Small Business	Small Business Administration
State & Local Governments	FEMA
State-Administered Federal Programs	Office of Management and Budget
Transportation	Department of Transportation
Tribal Governments	Department of the Interior
Wastewater Treatment	Environmental Protection Agency

ICC Sector leads, and their supporting staff, were responsible for maintaining continuous understanding and current status information on their sector during the Y2K rollover period. In performing these duties, they reviewed Information Collection and Reporting System (ICRS) status reports, obtained relevant information from their respective organizations through telephone conversations, faxes and e-mails, and reviewed media reports. Each sector also provided periodic summary reports of its status.

6.1 Lessons Learned – National Y2K Information Coordination Center (ICC)

On 19 June 2000, the National Y2K Information Coordination Center published its own list of 39 Best Practices and Lessons Learned from the Y2K effort. These are highlighted in Table 13.

Table 13: National Y2K ICC Best Practices and Lessons Learned

Best Practices
Most Important: 1. The leadership must have a vision, communicate that vision to all parties involved, and support people in its development and implementation. 2. Build a team of good people with requisite skills for the job at hand. Assign missions but give latitude and encourage creativity in accomplishment. 3. Take care of people. In addition to providing them clear direction and two way communications, this includes providing quality equipment and support to do the job at hand – fast machines, a reliable network, a friendly software environment, physical security (especially important when terrorist actions are a concern), provisions for emergencies, clean restrooms, safe parking, convenient restaurant facilities and updates on circumstances as they develop. People want to know what's going on and be part of the success. 4. Establish principles and policies which support teamwork and mission accomplishment. Important elements of the Y2K success included the following: - Integrity is non-negotiable - Questions are fair - Use existing agencies and capabilities; supplement where needed - Federal Response Plan is the model - One voice to the nation 5. Establish and maintain two-way communications. All-hands meetings were held periodically to update all on progress and frequent staff meetings were held to coordinate general direction. The director visited the working areas daily.

Table 13: National Y2K ICC Best Practices and Lessons Learned (continued)

Best Practices
Information Technology: 6. Use functional requirements as the basis and allow the support personnel maximum flexibility. 7 Involve users as early and continuously as possible in the development. The ICC established steering committees for Information Requirements and Public Affairs to ensure that the agencies were part of the development process, as well as implementation. It also hosted workshops with the states and agencies to introduce concepts, discuss, get feedback and train. 8 Establish architectures: - ***Operational*** – what you want to do and how you want to do it from a functional perspective - ***Information*** – what information is necessary to support the operational concept, where does it come from, and where does it need to go. May also address presentation format. - ***Technical*** – the infrastructure required to support the movement of information. Infrastructure may be dedicated or common use. The Pathway is not important; information appearing when and where it is needed is important. 9. Establish and use a configuration management process with all interests represented to prioritize requirements, control changes and coordinate work efforts. Keep minutes, use plain English and track status. The ICC Configuration Management Board met whenever requested, often on short notice to provide expeditious resolution. 10. Provide quality and high capacity equipment and tools to your most important asset – your people. The most common efficiency failure is to give programmers slow, memory limited equipment to develop on, so the programmers consequently spend time waiting for the machine rather than designing and writing code. Similarly, action officers should not have to wait for screen response when they have problems to solve. 11. Use state-of-the-art, but not bleeding edge, technology. The ICC made extensive use of mainstream equipment and software for ease of training, maintenance and interoperability. 12. Use the KISS principle. A simple plan, well executed, is much better than a complex plan that fails. The ICC used the web and a distributed database for much of its communications. Use of common browsers as the user interface minimized the training necessary for the agency, state and local users. The database approach allowed separate focus with the users to get the data in and gave great flexibility in formatting and displaying the information in useful form, to include setting thresholds and routing information of interest directly to the agencies. It was also much easier to install, maintain and troubleshoot than multiple stovepipe systems. 13. Be bold and create new capability when you need it. There was no existing system to know the status of critical infrastructure or system operations throughout the country. The ICC developed a web-based standard reporting system with easy assessment criteria that also served as a model for private infrastructure and international reporting. 14. Test, verify and validate throughout. All software was tested prior to putting it on line and systems were tested with the staff before the user community was brought in. The Independent Verification and Validation (IV&V) contractor and the National Security Agency were independently asked to attempt to hack our system in advance of operations to ensure security, readiness and training. 15. Do IV&V and make it constructive as well as evaluative. The time frame was very compressed. Rather than bringing the IV&V team in after the development was completed as is conventionally done, the IV&V team was brought in early and charged to comment and make suggestions as development progressed. Management determined whether or not to implement suggestions, thus maintaining control and responsibility, as well as the independence, of the IV&V team. Since the team was on board throughout, it had better understanding and required less lead-in time, and management had the benefit of its work much earlier in the process, and in time to make changes as necessary.

Table 13: National Y2K ICC Best Practices and Lessons Learned (continued)

Best Practices
Information Technology (continued): 16. Make instructions user friendly, timely and easily available. Electronic copies were provided by e-mail and in the on-line help files, as well as illustrated desk folders in the Operations Center. Feedback was sought and instructions were expeditiously updated accordingly. Good stand-alone instructions are difficult to accomplish the first time out, and feedback is essential. 17. There MUST be a Network Operations Center and it MUST include expertise in communications, automation and the specific applications that are being used, be operational early, have established metrics for each application (just like doctors measure your vital signs) and be proactive in knowing everything about the complete IT system, not just its components. If a problem occurs, network management needs to ensure that representatives of all functional areas involved are working the problem to avoid a serial, lengthy, finger-pointing process. Many of the ICC people had only worked component level, but the value of the Network Operations Center (NOC) was instantly recognized once it was in operation. 18. Shifts should be scheduled and enforced. People do not recognize their own bad judgment when overtired. Actions and lessons learned need to be passed on to the next shift and institutionalized.
Operations: 19. Organize and provide space and support for the functions being accomplished. Sectors were grouped by Vital Mission Areas, so that the groups of people expected to have the most interaction would be close to each other physically, and would provide all staff virtual access to the same information. Ample and convenient conference rooms were provided with installed workstations and video teleconferencing for breakout or small group actions as required. Traveling profiles allowed access to all data, including individual e-mail, wherever an individual worked or moved in the Center. 20. Assign responsibility and authority to the levels where the work is done. Sector leads were charged with the responsibility for initiating actions in their area and for maintaining a current Sector Status Summary at all times. They were the experts for their area and were expected to do what was necessary without waiting for central direction. The Direction Center did give overall guidance, but principally was responsible for ensuring the sectors had what they needed to do their job. 21. Support the people doing the work. Sectors were the building blocks of the ICC information flow. All other activities supported the sectors. The Sector Status Summary was the baseline used for all actions – management, coordination with agencies and private sector, source material for the Public Affairs officers (validated data only), updates to decision makers and Congress, and historical archiving. Administrative support was provided to do all the consolidation and administrative work to allow the sector officers to focus fully on gathering and summarizing information, coordinating, and maintaining the Sector Status Summary. 22. Train and exercise people in mission-focused support capabilities and operations. Basic training was conducted in which users were walked through each of the IT support capabilities including office automation, e-mail, the Decision Support System, map displays and desktop video-conferencing. These skills were then exercised and introduced into operations using scenarios to exercise each skill. The ICC conducted a stressed exercise with many events, many of which crossed sector boundaries and required inter-sector coordination. To assist in focus, an outline by time zone (Midnight Express) of both potential problems and positive benchmarks was prepared to watch for as midnight and then business hours moved around the world. This included special note of midnight at Greenwich Mean Time (7:00 PM EST), when major operations entered the year 2000 (the Federal Aviation System and most global computer networks, as examples). 23. Create win-win situations. Reporting status placed some burden on each of the entities involved. By participating, however, the entities (including local level government and the private sector) gained access to ICC status reports on Federal agency operations and critical infrastructure, the media briefing points and early warning information.

Table 13: National Y2K ICC Best Practices and Lessons Learned (continued)

Best Practices
Public Affairs: 24. Be open, accurate and timely. One voice to the nation demanded coordination. The ICC routine briefing information cycle was two hours or less, with provision for inserting late-breaking information. Public Affairs officers from the agencies prepared the briefing bullets for their functional areas. Source-validated data proved accurate and the ICC added the credibility of confirmation and official release. 25. Coordinate press briefings and releases. In order to present one voice to the nation, agencies were asked to coordinate releases in advance. In general, facts were reported as they became known, and the agencies reported on response. Agency-released data was released simultaneously as well from the Joint Public Information Center to gain wider coverage. 26. Support the media in doing their job. A media center was provided with adequate working space to file and convenient access to our briefing studio. All questions were answered. Multiplex boxes were provided in the briefing studio and the media center to support the media with live feed for recording and transmission. ICC-unique press passes and use of the White House credentialing model facilitated quick entry. Simple measures like convenient soft drink and snack machines, clean restrooms and available round-the-clock restaurant facilities supported media focus and efficiency. 27. Provide information to Public Affairs Officers (PAOs) proactively. PAOs need good and timely information to be effective in informing the public. The PAOs had access to the current Sector Status Summary at all times. A consolidated summary was provided to all PAOs two hours prior to each scheduled briefing to enable them to structure the issues in appropriate format for timely review by ICC personnel prior to briefing.
Lessons Learned
28. The ICC was able to receive information from local through Federal governments and the private sector, domestic and international, and provide it to decision makers and to the public in a timely and accurate manner. The media acknowledged us as the authoritative source. 29. The interagency processes and cooperation worked, were exercised and were available for action as required. The Secure Compartmented Information Facility with appropriate circuit access and classified video-teleconference capability and co-location of the Catastrophic Disaster Response Group would have facilitated coordination with the appropriate decision makers had things not gone well. 30. The training and exercises adequately prepared operations personnel for the Millennium Rollover. In presenting more challenges than the actual rollover, the stressed exercise trained people, validated the support architecture, confirmed procedures, developed teamwork and instilled confidence on the part of all concerned. 31. Properly led and supported people get the job done. 32. Stakeholders buy in when they see need and benefit. The ICC was able to mutually make this a win-win for all concerned. 33. User focused and friendly IT support paid off in user acceptance and efficiency. 34. The web and database approach was relatively quick to develop and install and was exceptionally reliable. Firewalls intercepted probes and precluded hacking. 35. The functionally-based operational, information and technical architectures were sufficiently flexible to change and expand as increased demands were placed on them. 36. Plain English business rules controlled through a configuration management board are an efficient way to obtain mutual understanding between users and developers and ensure requirements are met. 37. Some states had automated reporting systems with their subordinate elements in place. Most did not. 19 states and 8 agencies requested copies of the Information Collection Reporting System software (The ICC provided documented copies for use on Solaris and NT copies to states and agencies). 38. Budget is always on the critical path. A principal factor for the ICC success was that, once selected, the prime and IV&V contractors began work at risk immediately. 39. The GSA Single Point of Contact was very helpful in both the stand up and close down of the Center.

6.2 Lessons Learned – International Y2K Cooperation Center (IY2KCC)

Since 1 January 2000, one of the most common themes of Y2K lessons learned from both the public and private sectors has been the in-depth awareness by managers and users of an organization's dependency on information technology and of the interdependencies among organizations, commercial vendors and systems.

The global Y2K experience created a unique opportunity to learn about how the world works, how international cooperation can be improved, and what vulnerabilities may remain. The "Report of the International Y2K Cooperation Center (IY2KCC) – Y2K: Starting the Century Right!" identified 18 general lessons learned across three categories, summarized in Table 14. Details of these lessons learned, as taken from the report, follow. These three categories are:

- Strategic
- Information
- Management

Table 14: Post-Rollover General Y2K Lessons Learned

Lesson No.	Category	Description
1	Strategic	A common menace and cross-border interdependencies were keys to success
2	Strategic	Networking and information cooperation work
3	Strategic	Leapfrogging is good
4	Strategic	Infrastructures are both connected and resilient
5	Strategic	Leadership is vital, but institutional agility varies
6	Strategic	Public-private partnerships can work
7	Strategic	Technology can be managed
8	Information	Facts build confidence
9	Information	Value self-reporting
10	Information	Close is better
11	Information	Details count
12	Information	Beware of information lag
13	Information	Information cartels have marginal value
14	Management	Explain the program in "plain English"
15	Management	Information and communications technology is mission-critical
16	Management	Know your systems, suppliers and business processes
17	Management	Manage risks proactively
18	Management	Prioritize requirements for results

According to the IY2KCC, the event produced seven lessons about solving international technology problems (***strategic***).

- **A common menace and cross-border interdependencies were keys to success**

  Unprecedented international cooperation made the outcome successful. Two attributes of Y2K made it so. First, Y2K threatened every nation, providing incentive to share best practices and reduce the total cost of fixing the problem. The immovable deadline of 1 January 2000 emphasized the nature of the menace. Second, it was of limited value for one country to solve its own Y2K problems if a neighbor on whom it depended for critical services or supplies was unable to function because of Y2K failures. This interdependency created a great deal of interest in mutual assistance so that every country was successful.

- **Networking and information cooperation work**

  The Y2K problem showed that, given incentives to cooperate, a combination of personal contact supplemented and sustained by electronic information sharing can create a virtual organization that works together to successfully solve a difficult problem. While a central organizing function need not be large, it is helpful to encourage the open exchange of quality information among network members.

- **Leapfrogging is good**

  Some nations/organizations started working on Y2K issues much later than others, but no significant difference in outcomes was apparent. A critical factor for this was that the cost and time to fix the problem decreased rather rapidly. Costs of implementation fell as automated Y2K tools became extremely accurate and efficient at fixing software code. As the Y2K mitigation process evolved, awareness increased that serious Y2K risks were confined to a small number of situations. Due to information sharing, late starters did not need to recreate the work of those who had tested all of the systems before them. Technology and knowledge advances can permit this type of beneficial "leapfrogging".

- **Infrastructures are both connected and resilient**

  There was pre-rollover concern that local Y2K failures would cascade around global interconnected power, communications and trade networks. The Y2K effort provided many lessons regarding supply chains and interdependencies. Y2K contingency planning and testing strengthened the ability of infrastructure operators to continue service in the face of technical problems. The success of Y2K increased confidence that many critical infrastructures would be able to recover from other kinds of attacks.

- **Leadership is vital, but institutional agility varies**

  Demonstrated leadership by formal institutions, including governments and multilateral institutions (e.g., United Nations, World Bank) was essential to Y2K success. In many cases, however, that leadership was demonstrated by individuals who were willing to move forward in the face of an urgent problem without undue regard for normal, formal channels. There were demonstrated benefits of establishing international communications on a non-political level to accomplish a goal with global implications, without the usual, formal red tape. In some cases (i.e., to approve the expenditure of funds) formal channels were necessary. The ability of institutions to make things happen quickly enough to be relevant to fixing problems varied greatly.

- **Public-private partnerships can work**

  In many sectors, public and private sector organizations worked together to solve Y2K problems. Private sector resources joined hands with governmental authority and sponsorship to leverage the best qualities of each. The international experience and analogous partnerships within many countries showed a convergence of private and public interests when faced with a threat that would potentially affect entire industries.

- **Technology can be managed**

  One of the most reassuring aspects of the outcome of Y2K efforts was its demonstration that the world community could organize itself across boundaries to manage problems in the technology that it has created.

- **Facts build confidence**

  The key to maintaining public confidence that the Y2K problem was being suitably addressed was the release of detailed readiness information, including what systems were ready, and what contingency plans had been made to ensure continuity of service where systems might not be ready. In some cases, information voids developed that were filled with rumors and self-serving predictions. It proved costly in time and frustration to reverse public perceptions of Y2K readiness when these voids developed.

- **Value self-reporting**

  Almost invariably, the outcome predictions of national Y2K coordinators were more accurate than those of external organizations. Many of these external organizations dismissed coordinators' statements as self-serving, aimed at promoting the best possible story to prevent public reaction. Coordinators, however, would be held accountable for their statements by the public and,

realizing that a misled public would react more unpredictably than a prepared public, erred on the side of caution with their pronouncements.

- **Close is better**

  A corollary to the value of self-reporting was the reliability of sources close to the problem. People or organizations having close proximity to a specific potential problem had a better vantage point, and, therefore, were able to provide more accurate assessments regarding whether a problem existed or not.

- **Details count**

  One frustrating aspect of much of the published Y2K information was its generality. The knowledge of facts and details regarding the actual effects of potential Y2K "failures" was critical to the absence or presence of dire predictions regarding consequences of systems not being ready by those without direct responsibility for solving the problem. Where these facts and details were not known by outsiders, unnecessarily pessimistic opinions regarding the impact of the Y2K rollover predominated.

- **Beware of information lag**

  Information takes time to become public. The normal process of gathering data and preparing, summarizing and checking reports prior to publication means that public, government, or organizational reports may contain status information that is weeks or months old by the time they become public. As the rollover date approached, there was less emphasis on creating reports and increased focus on completing fixes. As a result, implementation schedules were met, but public information on status became stale.

- **Information cartels have marginal value**

  The majority of the Y2K coordinating or evaluating bodies, whether official or private-sector, developed detailed databases containing information about product, system or country readiness. Most private organizations did not share data with outside entities due to liability, security or proprietary reasons. Possession of these details permitted those with access to the information to better focus their efforts at specific system levels (e.g., medical devices). At the organizational level (such as airports), however, the quality of the privately-held information was generally no better (and at times less accurate) than the information available to the public.

- **Explain the program in "plain English"**

  Those involved with the Y2K effort around the world learned how to communicate an apparent technology problem as a business and management

problem. This led to explanations of a technology failure in terms that organizational leadership could understand. At the national level, coordinators learned that, in order to influence global economic and media organizations, significant focus was needed to ensure that readable English-language versions of their readiness reports would reach opinion leaders.

- **Information and communications technology is mission-critical**

  Management at all levels learned how dependent their organizations are on information and communications technology. For many organizations, their internal systems, those of their suppliers and customers, and the infrastructure itself, were at some risk from Y2K.

- **Know your systems, suppliers and business processes**

  Y2K "encouraged" organizations to produce comprehensive inventories of their critical systems, as well as those systems' functions and interconnections. For many organizations, this constituted the initial creation of an inventory. At the international level, many countries used Y2K to improve the coordination of emergency response mechanisms. In a similar vein, both organizations and countries gained a much better understanding of who they rely on for supplies of critical goods and services. Finally, knowledge about systems and suppliers fed into a broader understanding within organizations as to the need to know how an organization actually performs its "missions". The Y2K effort revealed many intricate processes and interrelationships that had historically evolved, providing a unique opportunity to understand and improve them.

- **Manage risks proactively**

  Two key benefits derived from the Y2K experience include (1) the usefulness of preparing for service interruptions and (2) the importance of testing, not simply producing, contingency plans. It also underscored the benefits associated with communication with the public, both early and often, regarding matters of potential widespread concern, rather than reactively waiting for and responding to those concerns.

- **Prioritize requirements for results**

  Ultimately, what counted was not whether all of the minor Y2K bugs were fixed, but whether critical services continued to be delivered, without interruption. The overall measured strategy of devoting significant resources to tackle the critical infrastructure first, and saving less critical problems for late, worked exceptionally well.

6.3 Lessons Learned – Center for Y2K & Society

Just after the rollover, the Center for Y2K & Society published interim findings from their Y2K Impact Monitoring Project, which was a proactive outreach campaign to assess the Y2K post-rollover status of healthcare, environmental and social service organizations nationwide. Respondents cited the results shown in Table 15 as benefits, observations and lessons learned resulting from their Y2K preparations.

Table 15: Benefits, Observations and Lessons Learned from Y2K Preparations (Center for Y2K & Society)

Benefit	Comments
Hard Deadline Forced Action • Forced Disaster Preparedness • Focused Attention on Needed Improvements • Demanded Individual and Organizational Action	Y2K represented a hard deadline of 31 December 1999, by which all organizations had to ensure compliance. • Organizations and communities had to re-examine their disaster contingency plans • Outdated technology was upgraded and insufficient inventories were improved • The immovable deadline forced people to overcome resistance once the Y2K business case was presented to top leadership
Increased External Communication and Collaboration • Created New External Communication Channels and Improved Existing Ones • Identified Key People and Fostered Relationships With Them • Provided Increased Visibility of Non-Profits	Y2K preparedness efforts highlighted the need for cooperation among organizations and their respective stakeholders. • Organizations had an opportunity to develop relationships with community leaders through meetings, forums and conference calls • Respondents noted that the funding increases that they received to address Y2K problems provided an additional benefit of increased exposure for their organization
Prompted Internal Organization Improvements • Increased Non-Profits Volunteer Base • Created More Effective Internal Communications Systems • Mandated More Efficient Technological Systems • Highlighted the Need for Resourcefulness within Individual Organizations	Y2K provided organizations with an impetus to evaluate themselves and their operating systems • Many respondents noted that new volunteers who aided in their Y2K preparation efforts remained involved in the program after the rollover • Many organizations established clearly-defined staff roles and communication methods in case of disaster • The need for Y2K-compliant hardware and software led to increased efficiency for many organizations • Non-profits had to find ways to make the most of their limited financial resources in order to prevent an interruption in services to those dependent on them

Table 15: Benefits, Observations and Lessons Learned from Y2K Preparations (Center for Y2K & Society) (continued)

Lesson Learned/Observation	Comments
Increased Awareness of Societal Interdependence	The existence of so few, relatively minor Y2K-related problems is an indication of the committed and collaborative efforts of numerous individuals and groups nationwide. The Y2K success demonstrated what can be achieved when people work together to achieve a common goal.
Provided a Model of Government Facilitated Action	Government outreach at all organizational levels spearheaded widespread Y2K preparation efforts with little or no need for legislation or regulation. The President's Council on Y2K and the community preparedness groups are two examples that can be cited as "best practices".
Emphasized the Need for Internal Organizational Assessment	The Y2K experience provided an imperative for organizations to conduct a self-assessment of their staff, technological resources and disaster preparedness that all organizations should undertake on a periodic basis.
Highlighted Widespread Technological Vulnerability	Y2K was a prime example of how dependent society has become on technology. The fallibility of computer systems has been recognized, as has the importance of having contingency plans in place should those systems fail. A further lesson is to not take the critical infrastructure for granted.

6.4 Lessons Learned – Federal Funded Institutions Examination Council (FFIEC)

The Federal Funded Institutions Examination Council (FFIEC) published its own set of lessons learned from the Y2K experience, determining that the best-prepared institutions possessed most or all of the following characteristics:

- **Senior Management/Director Involvement and Interdisciplinary Teams**

  The commitment/involvement of senior management and board of directors from the early stages of the Y2K effort through its completion was critical to ensuring that all aspects of the project were carefully considered and that the project was clearly defined, supported, funded and monitored. Many institutions established new reporting mechanisms to keep senior management advised and to manage risks, helping to keep the project on schedule and supported with adequate resources. Quality assurance reviews, benchmarking and internal audits were established to ensure proper risk management. Some institutions established clearly-defined measurement objectives and conducted periodic reviews to ensure that goals and standards were met.

  The efforts of interdisciplinary teams comprised of experts from IT systems, affected business units, law departments and corporate communications helped institutions to better manage risks, facilitate critical phases of the project and emphasize the priority of the project throughout the organization.

- **Comprehensive IT Inventories**

  Financial institutions developed current inventories of IT systems and applications, enabling many of them to consolidate, eliminate or integrate technology projects on an enterprise-wide basis. Effective planning helped in modernizing computer systems and integrating new systems with relevant legacy systems. These comprehensive inventories also fostered more effective risk evaluation and decision-making, ensuring that the IT systems were consistent with the institution's current operating strategies.

- **Improved Vendor Management**

  Financial institutions developed better due-diligence processes to oversee service providers and software vendors that provide mission-critical services and products. Many institutions found significant risk exposures related to vendor management that was not adequately measured, monitored, managed or controlled. As a result, they expanded their analyses of these suppliers to fulfill contractual obligations, and took steps to improve communications and clarify roles, responsibilities and contractual requirements.

- **Effective Testing Strategies**

  Formalized strategies improved the Y2K testing process by recognizing interdependencies between IT systems and other business units. Many institutions had developed these strategies for the first time. Testing environment and processes were also improved by creating more efficient testing methodologies and change-management practices.

- **Detailed Contingency Planning**

  Significant benefits were reported from the development and implementation of Y2K contingency and "event management" plans. Contingency planning evolved from theoretical exercises to a problem-solving and training tool to help organizations respond promptly to operational failures and natural disasters. More detailed contingency plans were developed by (1) analyzing the effect of potential system failures on core business processes, (2) determining the minimum level of output and services for each core business process, (3) testing the contingency plans (actions and responses), and (4) validating the results through independent parties. Institutions also recognized the need to review and plan for contingencies related to all aspects of their operating environment, including IT systems (e.g., mainframe systems, desktops, networks) and non-IT systems (e.g., facilities, buildings). Simulations, "table top" exercises and other forms of tests reduced the time needed to respond to operational problems and improved communications and decision-making among senior management, corporate communications officials, and business units.

- **Strong Internal Controls and Security**

  Attention was focused on protecting critical IT systems by establishing better safeguards to detect fraudulent, malicious and negligent acts from both internal and external sources. Control points included satisfactory internal audits of facilities, personnel, policies/procedures, telecommunications, system/application software, service providers and software vendors. Important precautions to protect system security included (1) enhanced security access restrictions, (2) background checks on employees and contractors, (3) enforcement of appropriate separation of duties, and (4) generating effective audit trails. Institutions also developed contact lists to obtain advice on how best to respond to intrusions/attacks on computer and telecommunications systems, and then to alert others.

- **Open Information Sharing**

  The Y2K effort provided a unique demonstration of cooperative and open communication among individuals and corporations across competitive lines and regulatory boundaries. Financial institutions worked together with other institutions, service providers, software vendors, trade associations, regulators and other industries to share information and strategies, and to respond to media reports or perceptions that could negatively impact public perceptions or Y2K preparedness.

  Examples of stakeholders in information sharing efforts included:

  - The public and community at large
  - Law enforcement
  - Government agencies
  - The national security and intelligence communities
  - Providers of network and other key infrastructure services
  - Technology and security product vendors
  - Security experts
  - Incident response teams
  - Education and research communities
  - International standard-setting bodies
  - Media

- **Improved Public Relations**

  The Y2K effort afforded many opportunities to communicate with customers, either building on previous relationships or establishing new relationships. The financial industry took great steps to ensure the release of accurate information to the public regarding Y2K readiness.

- **Thorough Legal Review**

  Many institutions benefited from the involvement of legal council on their Y2K project management teams. Based on legal counsel review of contracts as part of the vendor management process, some institutions were able to avoid contractual issues with service providers and software vendors. Many institutions also established consistent approaches for documentation retention and record keeping as part of their legal defense strategy for demonstrating Y2K due-diligence. In-house counsel also benefited from working closely with Chief Technology Officers and Chief Information Officers on a project that cut across a range of different disciplines.

6.5 Lessons Learned – Federal Agencies and Departments

The Y2K effort represented a huge risk management exercise. From the enterprise level to individual projects to specific software applications, the risks needed to be identified and mitigated. Now these processes and procedures developed by the agencies for identifying Y2K risks can be applied to other enterprise projects. After Y2K, agencies should now have the information and relationships to look at critical infrastructure protection from an enterprise-wide strategic planning point of view, rather than each individual office trying to attack problems.

Building enterprise architectures, innovating delivery of services, protecting critical systems, and conducting strategic capital planning are all part of good management of the Government's IT dollars and investment in infrastructure protection. The risk is to go back to business as usual. The Government made a significant investment in Y2K. Agencies need to keep looking ahead to leverage how they can extend the benefits of that investment.

From a big-picture, IT perspective, the Y2K effort provided Federal agencies with the opportunity to make more strategic IT capital planning decisions and identify where to make the right IT investments so that redundancies could be eliminated and economies of scale could be leveraged. Many e-Government implications also came out of Y2K, helping agencies consider how they can better use IT to deliver services and conduct business over the Web.

In its Final Report, "The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion", dated 29 March 2000, six basic principles were listed as being demonstrated by the Y2K experience:

- **PRINCIPAL 1:** Top management needs to be involved in information technology decisions on an ongoing basis
- **PRINCIPAL 2:** Organizations need to do a better job of keeping track of and managing the technology they use, and the functions that the technology performs
- **PRINCIPAL 3:** Contingency plans should be continually updated and tested
- **PRINCIPAL 4:** Industry National Centers are an important resource for reconstitution of critical services
- **PRINCIPLE 5:** Full disclosure is critical to sustaining public confidence in the face of possible emergencies
- **PRINCIPLE 6:** Forming partnerships across traditional boundaries can be a tremendous asset in the drive to achieve a commonly held goal

In September of 2000, a report entitled "Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges" (GAO/AIMD-00-290) was submitted to the House Subcommittee on Government Management, Information and Technology and discussed several Y2K lessons/benefits that could be applied to future management challenges, such as critical infrastructure protection. These lessons/benefits included:

- **Leadership/partnerships were key to the nation's successful Y2K oversight and coordination**
    - Congress played a key oversight role
    - Central leadership and coordination of the Federal Y2K effort was invaluable
    - The value of partnerships was often cited as an important Y2K lesson
    - Many methods facilitated communications among partners and others
    - Human capital and budget initiatives were important

- **Agency Y2K efforts resulted in improved Information Technology management**

    - Agency Y2K actions benefited from high-level management involvement
    - Risk analysis allowed agencies to prioritize work
    - Improved project management practices were implemented
    - Inventories and configuration management processes were improved
    - Independent reviews provided valuable management information
    - Y2K work led to development of reusable testing practices
    - Business continuity and contingency plans were beneficial

- **Sustaining Y2K momentum is critical to achieving success in other management challenges**

    - Critical infrastructure protection and security
    - Effective use of technology
    - Large-scale IT investments
    - Updating/developing IT management policy and standards (security; e-government)

In May 2001, the U.S. Department of State, Office of Inspector General issued its own take on lessons learned from the Y2K effort. Entitled "Year 2000 Lessons Learned: Strategies for Successful Global Project Management", it provided an overview of six key principles representing a framework for discussion of the successful practices and lessons that were identified as part of the State Department's Y2K review. These principles were touted as providing specific areas of focus for ensuring successful global project management. They are summarized in Table 16.

Table 16: Matrix of Applied Year 2000 Lessons Learned from "Application of Y2K Lessons Learned" Audit Report (Report No. D-2001-175)

Organizational Relationships	Information and Technology Management	Human Relations
PRINCIPLE I: Recognize Leadership and Commitment as Keys to Success	**PRINCIPLE III:** Exploit Opportunities for Management Improvements	**PRINCIPLE V:** Build Public Awareness and Confidence
PRACTICES: A. Understand the U.S. leadership role B. Optimize the contribution of key individuals C. Ensure senior-level involvement D. Provide adequate funding and commitment	PRACTICES: A. Recognize the importance of IT to business/mission accomplishment B. Be aware of the risks accompanying technological advancement C. Take advantage of opportunities to examine and improve business processes D. Improve systems management E. Emphasize systems testing and verification F. Enhance IT project management practices G. Recognize the importance of contingency planning and emergency preparedness H. Make innovative use of IT tools and techniques	PRACTICES: A. Manage fear B. Launch public awareness campaigns C. Institute public safeguards
PRINCIPLE II: Appreciate the Value of Coordination, Cooperation and Collaboration	**PRINCIPLE IV:** Coordinate Guidance, Monitoring, and Data Reporting and Analysis Activities	**PRINCIPLE VI:** Consider Cultural Differences
PRACTICES: A. Promote worldwide cooperation at all levels B. Form public/private partnerships C. Ensure legal and regulatory support	PRACTICES: A. Effectively support decentralized crisis management activities B. Improve guidance for field operations C. Eliminate redundant and burdensome reporting requirements D. Consolidate data collection activity overseas E. Synthesize analysis of data collected F. Coordinate monitoring and communication activities G. Make proactive use of audit organizations	PRACTICES: A. Look beyond Western perspectives and approaches B. Avoid misinterpretation of foreign approaches

The Final Committee Report of the U.S. Senate Special Committee on the Year 2000 Technology Problem entitled "Y2K Aftermath – Crisis Averted" identified three key lessons learned/benefits derived from the Y2K experience:

Modernized Technology Base and Management Efficiency:

The attention of executive-level personnel at vital stages of Y2K prioritizing, planning and remediation has resulted in higher levels of accountability and reliability in IT management. For the first time, and at a critical juncture in the development of an IT-driven economy, private firms and public organizations have been forced to look critically at the role of IT assets and to manage them as mission-critical resources.

Better Communication Networks and Public/Private Partnerships:

Trade associations were instrumental in the establishment of industry Y2K practice standards and in communicating results of compliance efforts. Industry groups, associations of public managers and trade organizations all established Internet websites that communicated levels of Y2K readiness, or mentored how members could become Y2K compliant. Internet use also provided an unprecedented level of organizational transparency that paved the way for effective public/private partnerships and open communication between different industries. International partnerships were also established, facilitated by the International Y2K Cooperation Center under the auspices of the U.N., with funding from the World Bank.

Greater Awareness of IT Dependencies and Security Risks:

Y2K prompted the Government and industry to closely examine the Y2K infrastructure upon which they rely. The revolution in e-commerce has perforated complex interconnected business entities with security breaches. Denial-of-Service (DoS) cyber-attacks in early 2000 raised questions about the security of websites, such that this threat to businesses should provide additional incentive for industry to work with Government to develop a common solution.

Specifically for the DoD, there have been many positive outcomes from the effort devoted to fixing the Y2K problem, including the following general benefits as a result of Y2K preparations:

- **An inventory of all IT systems.** In addition, the management structure is in place to effectively administer the approximately 9,900 systems in the DoD.
- **Improved procedures for managing IT assets.** There has been a significant increase in the awareness of configuration management as a Chief Executive Officer (CEO) issue related to mission performance.
- **More uniform and up-to-date versions of software throughout DoD.** Many long overdue upgrades were completed to achieve Y2K compliance.

- **A detailed mapping of, and agreements with, interfaced organizations.** The mapping shows where DoD relies upon others or is relied upon for data. It provides insight into determining the true costs of enterprise-wide upgrades.

- **A contact network is in place to deal with future enterprise-wide IT issues.**

- **The groundwork for network-centric warfare has been developed.** As a result of the efforts on Y2K, DoD is better prepared to deal with overt and covert attempts to undermine IT capabilities.

In addition, the DoD felt that the actions taken in preparation for the Y2K Date Conversion dramatically increased the visibility and criticality of both cyber and physical Critical Infrastructure Protection (CIP) throughout the Department. The Y2K effort within the DoD demonstrated the ability to:

- Understand highly complex (including cyber and commercial) infrastructure

- Identify single-points of failure

- Correct those vulnerabilities in an expeditious, affordable manner

Significant CIP efforts/results reported as of January 2001, as well as some lessons learned/benefits gained as a result of the Y2K effort, are summarized in Table 17. The Y2K effort demonstrated that the DoD has the potential to create an effective CIP program to protect both critical cyber and physical infrastructures and respond to the infrastructure challenges the Department is now facing.

Table 17: Summary of Significant DoD CIP Results/Efforts and Lessons Learned/Benefits Gained as a Result of Y2K (January 2001)

• The Secretary of Defense designated the Y2K event as a Defense-wide operational readiness issue
• DoD shifted its Y2K/CIP focus from systems and information technologies to an integrated cyber and physical infrastructure reliability and operational readiness approach
• Dramatically improved integration between DoD Chief Information Officers (CIOs), Chief Infrastructure Assurance Officers (CIAOs), Commanders-in-Chief (CINCs), the Services, Defense Agencies, the OSD staff, and the Department's senior leadership. DoD personnel worked together in integrated, Defense-wide teams to make information systems and physical infrastructures Y2K compliant and reliable to ensure the Department's worldwide operational readiness.
• Dramatically improved Defense-wide understanding of Department's dependencies on critical, domestic, host-nation, and international cyber and physical infrastructures which are beyond DoD control, yet are required to accomplish core DoD missions

Table 17: Summary of Significant DoD CIP Results/Efforts and Lessons Learned/Benefits Gained as a Result of Y2K (January 2001) (continued)

• Greatly reduced the risk of Y2K-induced infrastructure failures through creation of a series of risk mitigation measures that included requirements for 123 major/mission-critical system "End-to-End" evaluations, automated screening of computer software code, and strict configuration management policies and procedures
• Upgraded and improved information system, installation and operational contingency plans to ensure continuity of operations regardless of any Y2K-related infrastructure disruptions
• Given the global context of the Y2K challenge, the interagency infrastructure readiness and Consequence Management coordination processes were defined, refined, exercised and made available for any required action
• Jointly developed and executed Y2K/CIP and Consequence Management related training and exercise scenarios
• DoD operations personnel were prepared for the Century and Leap Year Rollovers by exercising a large number of infrastructure failure and consequence management challenges. These exercises very effectively trained people, validated response architectures, honed decision-making procedures, developed teamwork, instilled confidence, and ensured the maintenance of the global operational readiness of the Department.
• User-focused and friendly IT and collaborative tool support paid off in user acceptance and efficiency
• The functionally-based operational, information and technical architectures were sufficiently flexible to change and expand as increased demands were placed on them
• Plain English business rules, controlled through a configuration management board, were an efficient way to obtain mutual understanding between users and developers, and to ensure that requirements were met
• Built a strong consequence management policy
• Efforts were actively supported by leadership
• Made "infrastructure defenders" equal to Nuclear Command and Control, National Command Authority, and current Operations and Intelligence personnel
• Created the Decision Support Activity
• Integrated Information Assurance (IA) into CIP resources to provide global infrastructure and performance analyses to support DoD asset allocation, Consequence Management operations, and Senior Leadership decision-making
• "Operationalized" cyber and physical CIP in support of Defense objectives
• Integrated the DISA infrastructure monitoring and decision support efforts with those of the President's Information Coordination Center (ICC)
• Tasked, organized and trained the OSD Staff
• Provided direct infrastructure monitoring and decision support to the Executive Secretariat and Executive Support Center
• Introduced the Automated Collaborative Decision Support Tool to accelerate the DoD consequence management coordination and decision process
• Effectively integrated Contractor personnel and Reserve Component Officers into the infrastructure monitoring, decision support and Consequence Management roles
• Developed and initiated efforts to identify Logistics Sector physical and cyber assets building on the Y2K logistics end-to-end test planning process, focusing on those assets supporting logistics processes identified by the CINCs as critical
• Instituted new business processes to incorporate lessons learned from vulnerability identification. Lessons learned will be applied to information infrastructure upgrades and new technology insertions.

Table derived from "Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities", January 2001, http://www.ciao.gov/CIAO_Document_Library/final.pdf

The FY 2000 DoD Appropriations Bill directed the DoD to provide a report to the congressional Defense committees by 15 March 2000 on Y2K lessons learned, emphasizing which particular programs should be continued and what lessons could be applied to information assurance. The ASD(C^3I), Air Force and Joint Staff prepared these reports, while the Navy provided an undated document.

In its "Year 2000 (Y2K) Lessons Learned" report to the Congressional Defense Committees (dated 15 March 2000), the DoD indicated that there were many lessons learned from the Y2K experience at every echelon of DoD. The report distilled and grouped the most important of these into three categories:

- Enterprise-wide lessons applying to DoD and other Federal agencies
- Chief Information Officer (CIO) lessons that apply to DoD efforts to achieve compliance with the Clinger-Cohen Act of 1996
- Warfighting lessons learned from the Joint Staff and CINCs

These lessons learned and DoD-wide recommendations are described in Table 18.

Table 18: Summary of DoD Y2K Lessons Learned and Recommendations

Lesson	Discussion
Enterprise-Wide Lessons Learned	
Hard Work Paid Off (Everything Worked)	Across DoD, thousands of systems continued to function across the century rollover. Where there were problems, contingency plans also worked and assets were available to quickly respond to problems.
Government Worked	Interagency efforts coordinated by the President's Council on Y2K, including the Federal sectors and high impact programs, resulted in Y2K success. Cooperation between Government and industry worked, as did an unprecedented cooperation between governments.
Warfighting/Readiness Issue	In summer 1998, it was recognized that Y2K was a CEO problem, not just a CIO problem. The Secretary of Defense (SecDef) directed DoD leadership to treat Y2K as a readiness issue. This direction ensured that all members of DoD understood the need to cooperate to achieve Y2K success and galvanized Y2K preparedness efforts.
Horizontal Problems vs. Vertical Organizations	Whereas DoD and Government are vertical, problems such as encryption and Y2K are horizontal. The Y2K problem demonstrated the utility of standardized guidance and performance measurement tools to focus efforts across the organization, coupled with proactive external auditing and effective management response.

Table 18: Summary of DoD Y2K Lessons Learned and Recommendations (continued)

Lesson	Discussion
Enterprise-Wide Lessons Learned (continued)	
Increased Dependence on IT Systems	Business process improvements have increased dependence on IT systems, resulting in a potential vulnerability (e.g., "just-in-time" logistics). The DoD achieved Y2K success by teamwork with its business partners. The DoD required confidence in its business partners, which resulted from teamwork and other measures.
Importance of Computer Professionals	One important outcome was that warfighters realized that they needed the computer professional. After the Y2K effort, it was recognized that DoD needs to adapt to recognize the significance and contributions of IT professionals.
Importance of Effective Chief Information Officers	DoD CIOs must have a close working relationship with warfighters and senior leadership in order to make best use of IT. Since a high level of information technology supports every part of DoD, effective participation by the CIO in business decisions was clearly recognized by all. These efforts span the DoD business processes of warfighting; support operations; and organizing, training and equipping.
Collaborative Partnerships	DoD efforts in working with industry and allies had payoffs beyond Y2K. Increased appreciation for the level of interdependence and linkages of IT systems had major benefits for daily operations and planning. The Enterprise Software Initiative proved extremely successful in making quality assurance and test support software useful in Y2K compliance testing, code analysis, regression testing, and code quality assessment widely available throughout DoD.
Centralized Guidance/Decentralized Execution	The use of one capstone document, the "DoD Y2K Management Plan", to provide centralized policies, procedures and performance measurement tools was a key element of DoD Y2K success. The scope, magnitude and complexity of the DoD Y2K problem made decentralized execution a necessity. Making centralized guidance widely available online fostered teamwork and helped ensure that all organizational elements focused on the same goals.
Accurate Inventory of IT	Centralized visibility of assets (e.g., acquisition, configuration management and information assurance) is fundamental to IT management. Timely and accurate performance measurement is essential to quality management oversight. The DoD Y2K database was used to ensure visibility and standardized reporting of progress. By making the database available online to all DoD Components, including the Intelligence community, the reporting process was compressed, and allowed the database to be used as an accurate and comprehensive measure of DoD progress in many areas of Y2K. The database was used as the basis for compliance to Public Law 106-79, "DoD Appropriations Act for Fiscal Year 2000", concerning registration and certification of IT systems by the CIO.

Table 18: Summary of DoD Y2K Lessons Learned and Recommendations (continued)

Lesson	Discussion
Chief Information Officer Lessons Learned (continued)	
Teamwork with External Oversight and Audit Organizations	One of the major factors for DoD Y2K success was the transparency resulting from the involvement of Congress, GAO, OMB, and the DoD Inspector General in all aspects of the Y2K effort.
Warfighting Lessons Learned	
Overview	Dealing with Y2K required parallel execution of many parts of a complex process. Success was enabled by leadership; unprecedented close relationships between DoD, the Joint Staff, and the CINCs, Services and Defense Agencies and Activities; and a willingness and ability to re-focus workforces as the collective understanding of the Y2K problem evolved.
Joint Staff and CINCs	
• Rollover Organizations	• The use of well-staffed organizations paid off. A clear focus on Y2K failures, millennium groups and terrorist attacks, and computer network attacks was maintained and served well. During rollover reporting, however, it was clear that the current report formats work well for operational issues, but are not well structured for capturing the impacts of IT problems on warfighting operations.
• Use of Reserve Forces	• Reserves and contractor support were essential to the Y2K effort. Many individuals were called to active duty to support various aspects of the Y2K effort. Lead times and processes to obtain reserve forces varied among the reserve Components.
• Joint Staff and CINC CIOs	Based on work during Y2K, it became clear that CIO roles, responsibilities and implementations were inconsistent across the combatant commands and the Joint Staff. DoD is developing a plan of action to establish CIOs on the Joint Staff and CINC staffs.
DoD-Wide Recommendations	
Data Reuse	Many types of information and data were centrally located for Y2K, including OSD, Joint Staff, CINC, Military Department, and Defense Agency databases. The Y2K "thin-lines" and mission architectures provided a view of the critical processes and interrelationships of selected critical warfighting missions and tasks. Contingency plans and continuity of operations plans were developed. This data/information has many potential reuses, including information assurance; critical infrastructure protection; joint operational architectures; and refinement of deliberate and contingency planning. The data is also potentially useful for incorporating these areas, plus interoperability and configuration management, into military exercises; and for enhancing DoD IT management.
Management Process	The integration of CIOs and Warfighters was key to Y2K success. The construction of "thin-line" architectures provided valuable insights into warfighting tasks and the reliance on IT systems. Coupled with operational evaluations that tested system interoperability, the need to carefully manage IT systems supporting warfighting operations was realized. Based on this, the Joint Staff and CINCs will develop joint operational architectures for all warfighting mission areas.

Table 18: Summary of DoD Y2K Lessons Learned and Recommendations (continued)

Lesson	Discussion
DoD-Wide Recommendations (continued)	
Configuration Management	The CINCs require insight into their system configurations to allow analysis of the benefits and risks of fielding IT systems or configuration changes. The Joint Staff and CINCs will work to develop a framework for sustaining CINC insight into system configurations. Another Y2K success factor was the use of software tools to support configuration management and technical problem isolation. The tools are used on a daily basis and are required for future operations. DoD will renew licenses for IV&V tools for further use in configuration management. Another Y2K lesson learned by warfighting functional Components was that IT management programs are not well defined or adequately resourced, nor are program requirements fully defined. CINCs and the Joint Staff will continue working to ensure that IT managers fully define program requirements and that resources are provided once requirements are defined.
Testing	The warfighting context provided by CINC operational evaluations was critical to DoD Y2K success. Operational evaluations validated IT testing and evaluation, including examination of contingency plans. In the future, DoD will incorporate information assurance, critical infrastructure protection, interoperability, and configuration management issues into routine Chairman, Joint Chiefs of Staff (CJCS), CINC, and Military Department exercise and training programs. Another benefit of the Y2K effort was the appreciation of how battle labs added an invaluable dimension to CINC operational evaluations. These centralized testing facilities contained the necessary resources and expertise to enable successful IT testing of operational architectures.

Lessons learned from the ASD(C^3I) report, applicable to DoD and other Federal agencies, included (1) an increased awareness of the need to cooperate on cross-cutting issues, (2) the dependence on information technology systems, and (3) the importance of computer professionals. Lessons learned for CIOs included (4) the importance of partnerships, (5) the dependence on information technology systems, and (6) the need for an accurate inventory of information technology. According to this report, the DoD lessons learned provided a roadmap for improving information technology management that the DoD CIO would monitor for implementation.

According to the Air Force Year 2000 Final Report, the Air Force collected more than 400 Y2K lessons learned suggestions from the Major Commands, Direct Reporting

Units, and Field Operating agencies. They consolidated these suggestions into 60 lessons and recommendations. Key lessons learned included the need for improved resource management (including configuration management), procurement of independent verification and validation tools, implementation of code-scanning processes, a comprehensive information technology infrastructure database, and operational and system architectures at a system level.

Volume One of the Joint Staff Year 2000 Campaign Plan summarized 12 lessons learned that were presented to the Deputy Secretary of Defense by the Joint Staff Y2K Task Force Leader. The lessons included reusing data compiled for Y2K efforts for other information technology issues, incorporating information technology issues into routine exercises and training, and developing a prototype Joint Operational Architecture. According to this Year 2000 Campaign Plan, the lessons learned from the Y2K conversion process were to be maintained and used in future endeavors.

The Navy provided an undated document on Y2K lessons learned that summarized key findings of the Navy Fleet, Systems Command and Major Claimant representatives during a review to assess the reasons for success with Y2K conversion, and to capitalize on the Navy investment in resources for Y2K preparations. Some of the key recommendations included broadening the duties and responsibilities of the Navy CIO, establishing a methodology for obtaining and maintaining current configuration information, and continuing the development and expansion of land-based laboratory interoperability testing. The document also recommended that, as an enterprise, the Navy should embrace those initiatives and leverage the Y2K lessons learned to meet information technology challenges.

On 22 August 2001, the Office of the Inspector General for the Department of Defense issued an audit report entitled "Application of Y2K Lessons Learned" to assess how widely and successfully the DoD had applied the lessons learned from the Year 2000 conversion experience to other information technology programs and management issues. Since the rollover event, many DoD Components were identified as having adapted

management experiences gained from the Y2K effort, and having reused and updated data compiled during those efforts, such as system inventories, thin-lines, contingency plans and configuration management.

For the information reported directly to the "Application of Y2K Lessons Learned" Audit Report, Table 19 provides a matrix summary of the lessons learned by the audited organizations for the categories of data reuse, adaptation of management experiences, senior management involvement, and continuing partnerships. It should also be duly noted that, while the Joint Staff published 12 lessons learned in their "Year 2000 Campaign Plan, Volume 1, only 2 of the 12 lessons had been adapted as of August 2001.

Table 19: Matrix of Applied Year 2000 Lessons Learned from "Application of Y2K Lessons Learned" Audit Report (Report No. D-2001-175)

Agency/ Component PSA	Data Reuse					Adaptation of Y2K Management Experiences	Senior Management Involvement	Continuing Partnerships	Lasting Impact
	811 Inventory	Other Inventory	Thin Lines	CP/ COOPs	MOAs				
ASD(C^3I)	Yes	N/E	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Army	Yes	Yes	Yes	Yes	N/E	N/E	Yes	N/E	Sig
Navy	Yes	Yes	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Air Force	Yes	Yes	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Marine Corps	N/E	N/E	N/E	N/E	N/E	N/E		N/E	Sig
DISA	Yes	Yes	N/E	Yes	N/E	Yes	Yes	Yes	Mod
Army National Guard	Yes	Yes	N/E	Yes	N/E	N/E	Yes	Yes	Sig
Air National Guard	N/E	Yes	N/E	N/E	N/E	N/E	Yes	N/E	Min
Joint Staff	N/E	N/E	Yes	N/E	N/E	N/E	Yes	N/E	Sig
Health Affairs	Yes	N/E	N/E	Yes	Yes	Yes	Yes	Yes	Sig
Personnel	N/E	Yes	Yes	Yes	N/E	Yes	N/E	Yes	Sig
Com	N/E	N/E	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Logistics	Yes	N/E	Yes	N/E	N/E	Yes	N/E	Yes	Sig
Weapons Systems	N/E	N/E	N/E	N/E	N/E	N/E	N/E	N/E	N/E

Com:	PSA for Communications
CP/COOPs:	Contingency Plans/Continuity of Operations Plans
Min:	Minimal Impact
MOAs:	Memorandums of Agreement
Mod:	Moderate Impact
N/E:	No Evidence Provided of Lessons Learned Application
Sig:	Significant Impact
Yes:	Partial or Overall Application of Lesson Learned

Taken from "Application of Year 2000 Lessons Learned", Office of the Inspector General, Department of Defense, Report No. D-2001-175, 22 August 2001, http://www.dodig.osd.mil/audit/reports/fy01/01-175.pdf (Link active as of 8 February 2002)

Based on the DoD lessons learned from the Y2K effort, the Joint Staff reported that it intended to take the following actions in coordination with the CINCs and other DoD Components:

- Review suitability of Operational Reports for global IT reporting
- Streamline and standardize Reserve call-up procedures
- Develop a resource strategy for large-scale CINC IT operations
- Develop a plan to establish CIOs on the Joint and CINC staffs
- Institutionalize integration of CIOs and Warfighters
- Consider databases, "thin lines", and leftover documentation for reuse in information assurance, critical infrastructure protection, joint operational architectures, standing contingency plans, exercises, and IT management
- Develop prototype Joint Operational Architectures
- Propose framework for sustaining CINC insight into system configurations
- Renew licenses for existing IV&V tools
- Define IT program requirements and resources accordingly
- Incorporate information assurance, critical infrastructure protection, interoperability and configuration management into routine exercises and training

In order to effectively implement the actions outlined above, the DoD recognized that four aspects of the Y2K process would be vital to leveraging the Y2K lessons learned:

- Senior leadership must remain engaged in IT management
- Every level of management and operations must understand the warfighting processes supported by IT systems
- IT management requirements must be defined and understood at all levels
- IT management functions must receive enough resources to meet the requirements

A bulleted summary of some of the more "anecdotal" lessons learned from the Army, Navy and Air Force, as taken from Y2K-Status.Org; Lessons Learned from Army, Navy, Air Force Y2K Projects website (http://www.y2k-status.org/Notes/Y2K/defense/LessonsLearned.htm) (active as of 26 March 2002), is listed below.

Army

- Y2K failures that occurred were minor and quickly resolved
- Y2K testing was a major risk reducer of Y2K failures on January 1, 2000
- Test all PCs and servers even if purchased with a Y2K warranty
- Dry runs are essential prior to actual testing to ensure completeness and accuracy of evaluations
- Early formal Auditor involvement is recommended. Make it an integral part of the overall management strategy.
- Information distribution – Y2K Listserver and General Officer e-mail distribution
- Practice early retirement/replacement of marginal systems

Navy

- Focus should be placed on information superiority. Total asset visibility, critical infrastructure protection, and information assurance were cited as elements of such superiority.
- Information sharing is critical. The Navy had emphasized that all personnel, military and civilian, would be both "Y2K aware" and "Y2K ready".
- Priority for Navy Y2K activities was placed on mission-essential services including power, potable water, waste water, safety, and security

Air Force

- Focused on the process rather than on the systems (critical information flows and decisions)

- Y2K responsibility should be given to senior level management. Early involvement should be encouraged.

- Configuration management must be enforced to ensure that systems tested and certified as being Y2K compliant do not develop Y2K problems as a result of subsequent changes

- The Air Force Audit Agency's Management Advisory Service helped to get senior leadership involved as of result of boosting Y2K visibility. It was recommended that the Auditors be used to fix problems, not merely to report them.

- The "no additional funding needed for Y2K" attitude was a problem. In addition, competing requirements for dollars pushed Y2K down the priority list.

- Contractor support was critical for testing since the experience was not available within the units

- Recommendations include starting early, getting senior leadership involved, and focusing on the process/mission

7 Application of Lessons Learned to Critical Infrastructure Protection

7.1 Background

As the first global challenge caused by information technology, Y2K represented only the first test of the Nation's infrastructure assurance programs. By definition, information security is considered a much harder problem to manage than Y2K. With Y2K, the rollover deadline and necessary completion dates were known well in advance of the actual event. With information security, the nature of the threat, the instigator of the threat, and if/when attacks will occur is much more uncertain. Efforts to address the Year 2000 computing problem called into attention some important aspects of risks to the nation's critical infrastructure. In particular, it highlighted computer-based interdependencies and the vulnerability of these systems to disruption. It also underscored the need to develop awareness, cooperation and a disciplined management approach to address information technology problems. Potential failures due to Y2K highlighted the need to include a cyber-reconstruction component in owners' and

operators' infrastructure assurance programs. In that vein, the Federal Government's role must now ensure that various programs across industry and local and state governments can be implemented in a coordinated and effective manner nationwide.

The President's Commission on Critical Infrastructure Protection was the first national effort to address the vulnerabilities created by the new Information Age. The Commission was tasked to formulate a national strategy for protecting the infrastructures that the U.S. depends on from physical and "cyber" threats.

Critical infrastructures are those systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation. Critical infrastructures are defined to include:

- telecommunications
- electrical power systems
- gas and oil (production, storage and distribution)
- banking and finance
- transportation
- water supply systems
- government services (continuity)
- emergency services

The threat has been generically defined as "anyone with the capability, technology, opportunity, and intent to do harm". Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. Terrorists, insiders, disgruntled employees, and hackers are included in this profile.

The October 1997 Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures", identified new

vulnerabilities, shared threats and shared responsibility as the cornerstone of its recommendations.

New vulnerabilities include:

> **Information and Communication:** All critical infrastructures are increasingly dependent on information and communications. The most important impact and vulnerability for this sector is the increasing interdependency of the Public Telecommunications Network (PTN) and the Internet. The PTN is increasingly software-driven, and remotely managed and maintained through computer networks. Deregulation of the telecommunications industry will significantly increase the number of access points, thereby increasing attack vulnerability.
>
> **Energy:** The widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for control of energy systems provides increasing opportunity for disruption and serious damage through cyber-attacks. The exponential growth of information system networks that interconnect business, administrative and operational systems contributes to increased system vulnerability.
>
> **Physical Distribution:** While the vulnerabilities for this sector remain predominantly physical, there are emerging cyber-vulnerabilities as this sector relies increasingly on information technology to shorten lead times; route and schedule traffic; etc. The same vulnerabilities that impact the Information and Communications infrastructure also impact every facet of the transportation industry. The most significant of these is associated with the modernization of the National Airspace System (NAS) and the plan to adopt the Global Positioning System as the sole basis for radio navigation in the U.S. by the year 2010.
>
> **Vital Human Services:** Cyber-vulnerabilities in this sector include the increasing reliance on SCADA systems for control of the flow and pressure of water supplies. In addition, Government services are dependent on huge databases of a highly confidential nature that contain information on private citizens. The inconsistent practices and increasing technological challenges to security allow exploitation through cyber-vulnerabilities of these databases.

The DoD has noted that the Y2K problem represented only a subset of a much larger and more insidious threat to our national security – that of planned Information Warfare (IW) attacks on the U.S. critical infrastructure. In Appendix B of its "DoD Year 2000 Management Plan", the DoD expressed concern that the very nature of the Y2K testing, evaluation and renovation processes had the potential of actually increasing the vulnerabilities of the Defense Information Infrastructure (DII) and DoD operational

readiness to these growing and increasingly sophisticated types of threats. The Y2K remediation efforts were seen as potentially providing a "cover" to introduce and/or exploit existing vulnerabilities within any information system or network. Such vulnerabilities had been used in the past to compromise the information, information systems and networks that make up the DII.

On 22 May 1998, the White House issued Presidential Decision Directive (PDD) 63, "Protecting America's Critical Infrastructure", which built upon the recommendations of the President's Commission on Critical Infrastructure Protection. PDD 63 represents the culmination of an intense interagency effort to evaluate those recommendations and produce a workable and innovative framework for critical infrastructure protection. The President's policy, as stated in PDD 63, is designed to:

- Set a goal of reliable, interconnected and secure information system infrastructure by the year 2003, and significantly increase security to Government systems by the year 2000, by:
    - Immediately establishing a national center to warn of and respond to attacks
    - Ensuring the capability to protect critical infrastructures from intentional acts by 2003
- Address the cyber and physical infrastructure vulnerabilities of the Federal Government by requiring each department and agency to work to reduce its exposure to new threats
- Require the Federal Government to serve as a role model to the rest of the country for how infrastructure protection is to be attained
- Seek the voluntary participation of private industry to meet common goals for protecting U.S. critical systems through public-private partnerships
- Protect privacy rights and seek to utilize market forces, and to strengthen and protect the nation's economic power
- Seek full participation and input from the Congress

A new structure was set up within PDD 63 to deal with the challenge of protecting the critical infrastructure, as outlined below:

- **National Coordinator:** Scope will include not only critical infrastructure, but also foreign terrorism and threats of domestic mass destruction (including biological weapons)

- **National Infrastructure Protection Center (NIPC):** Located at the FBI, this organization will bring together representatives from the FBI, DoD, U.S. Secret Service, Energy, Transportation, the Intelligence Community, and the private sector in an attempt at information sharing among agencies in collaboration with the private sector. The NIPC will also provide the principle means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts.

- **Information Sharing and Analysis Centers (ISACS):** The private sector is encouraged to set up these centers in cooperation with the Federal Government and modeled on the Centers for Disease Control and Prevention

- **National Infrastructure Assurance Council:** This council will be drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan

- **Critical Infrastructure Assurance Office (CIAO):** This office will provide support to the National Coordinator's work with Government agencies and the private sector in developing a National Plan, as well as help coordinate (1) a national education and awareness program and (2) legislative and public affairs

In its "National Plan for Information Systems Protection – Version 1.0", dated January 2000, the Government proposed 10 programs for achieving three basic policy objectives for protecting the Nation's critical infrastructure.

The first objective is ***Prepare and Prevent.*** This objective covers those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and those steps that will build an infrastructure that remains effective in the face of such attacks.

The second objective is ***Detect and Respond.*** This series of programs covers those actions required to identify and assess an attack in a timely and effective manner, and then contain the attack, quickly recover from it, and restore affected systems.

The third and final objective is ***Build Strong Foundations.*** This series of programs outlines what the Nation must do to create and support the people, organizations, laws and traditions that will help to Prepare, Prevent, Detect and Respond to attacks on the critical infrastructure network.

Table 20 provides a summary of these 10 programs, including brief descriptions and the planned implementation and milestone targets for their completion.

7.2 Potential Threat Sources, Targets and Techniques

Potential threats are primarily expected to come from "external" or "cyber" sources, but there also exists the possibility of "insider" threats. The activities of Y2K allowed individuals, including Government employees, and those associated with Y2K testing, evaluation and renovation, to gain increased access to systems that were previously restricted to trusted personnel.

The globally interconnected and interdependent nature of modern information systems, and how they relate to our critical infrastructure, allows IW attacks and similar types of activities to be directed through the Internet at all Components of the DII from any location in cyberspace. Attacks can also be conducted using less sophisticated means, which can include the introduction of untrusted/corrupt utilities (including freeware); COTS software products (including upgrades); and "sealed, official" shrink-wrapped and theoretically "trusted" software. As an example, consider the security "holes" that were inherent in the recently introduced Microsoft Windows XP Operating System software, and the resulting scramble to try to plug those holes.

Table 20: Summary of the National Plan for Information Systems Protection

Program No.	Title	Objective	Description	Implementation & Milestone Targets
1	Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities	**Prepare and Prevent**	The Government and private sector must identify significant assets, interdependencies, and vulnerabilities of critical information networks to attack, then develop and implement realistic programs to remedy those vulnerabilities, while continuously updating the assessment and remediation efforts.	Feb 1999 – May 2003
2	Detect Attacks and Unauthorized Intrusions	**Detect and Respond**	This program installs multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers (first in DoD, then the Federal Intrusion Detection Network [FIDNet] in coordination with other Federal Agencies) will receive warnings from these protection devices, as well as Computer Emergency Response Teams and other means, in order to analyze the attacks and assist sites in defeating them.	FY 1998 – Jan 2001
3	Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law	**Detect and Respond**	This program assists, transforms, and strengthens U.S. law enforcement and intelligence agencies to be able to deal with a new kind of threat and a new kind of criminal, one that acts against computer networks.	FY 1999 – FY 2000
4	Share Attack Warnings and Information in a Timely Manner	**Detect and Respond**	This program calls for a more effective nationwide system to pass information in real time about cyber-attacks, including (1) improved Federal information sharing, (2) the creation of Information Sharing and Analysis Centers (ISACs), (3) removing barriers to information sharing, (4) sharing between FIDNet and JTF-CND, and (5) use of a National Security Incident Response Center (NSIRC).	Jul 1999 – FY 2000
5	Create Capabilities for Response, Reconstitution and Recovery	**Detect and Respond**	This program attempts to limit an attack while it is underway and to build the ability to deal with information attacks into corporate and agency continuity and recovery plans.	Dec 1999 – FY 2003

Table 20: Summary of the National Plan for Information Systems Protection (continued)

Program No.	Title	Objective	Description	Implementation & Milestone Targets
6	Enhance Research and Development in Support of Programs 1-5	**Build Strong Foundations**	This program systematically establishes research requirements and priorities needed to implement the Plan, ensures their funding, and creates a system to ensure that our information security technology stays abreast with changes in both the threat and in the overall information systems.	Jun 1998 – FY 2001
7	Train and Employ Adequate Numbers of Information Security Specialists	**Build Strong Foundations**	This program surveys the number of people and the skills required for information security specialists within the Federal Government and nationwide, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.	Jan 2000 – May 2002
8	Outreach to Make Americans Aware of the Need for Improved Cyber-Security	**Build Strong Foundations**	This program will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-attack.	May 1999 – Mar 2000
9	Adopt Legislation and Appropriations in Support of Programs 1-8	**Build Strong Foundations**	Develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation between the Federal Government, including Congress, and private industry.	None Given
10	Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data	**Build Strong Foundations**	This program is integrated with all of the previous 9 programs, and is making what is done in the protection of critical cyber-systems conform to Constitutional and other legal rights.	FY 2000

The full spectrum of potential "actors" who may be capable of mounting an Information Warfare attack include:

- Nation and non-nation state organizations, including those entities that are openly or potentially hostile to the United States, its Allies and coalition partners. The Y2K effort afforded them a potentially ideal opportunity to conduct attacks on DoD systems, had they the capability and the incentive to do it.
- Hackers (both foreign and domestic)
- Vendors and vendor employees (both foreign and domestic) who provide software and Information Technology services to the DoD
- Disgruntled employees (including Government and commercial service providers and vendors)
- Trusted and untrusted, well-meaning yet untrained, and otherwise mistake-prone individuals

Figure 2, taken from the U.S. Senate 100-Day Report on the investigation of the Y2K problem, illustrates the interrelationships between (1) the Y2K remediation effort, (2) existing software vulnerabilities and (3) increasing foreign warfare capabilities as they result in increased vulnerabilities to U.S. national security.

Figure taken from "Investigating the Year 2000 Problem: The 100 Day Report", United States Senate Special Committee on the Year 2000 Technology Problem, 22 September 1999, pg. 194.

Figure 2: The Relationship Between Y2K Remediation Effort and Increased Vulnerabilities

Figure 3, which is taken from the Year 2000 Annual Report entitled "Technology Collection Trends in the U.S. Defense Industry" and published by the U.S. Defense

Security Service, depicts the regions of the world from which information collection efforts reportedly originated during calendar year 2000.

This map denotes regions of the world from where collection efforts reportedly originated. The percentages indicate the level of collection activity reported in 2000. The map does not imply national level support of the collection activity. The collector may have based their operation in a third country to conceal intentions such as the ultimate end-user of the research or technology.

Figure taken from "Technology Collection Trends in the U.S. Defense Industry", U.S. Defense Security Service, Vol. VII, 2001, http://www.dss.mil/cithreats/2001_trend.pdf (Link active as of 8 February 2002)

Figure 3: World Regions From Which Information Collection Activities Originated (Year 2000)

Figure 4, taken from "Critical Foundations: Protecting America's Infrastructures", Final Report of the President's Commission on Critical Infrastructure Protection, October 1997, pg. 20, summarizes the perceived threat spectrum from cyber-attacks.

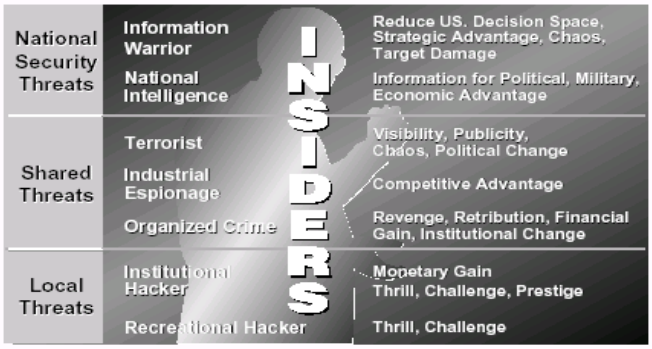


Figure taken from "Critical Foundations: Protecting America's Infrastructures", Final Report of the President's Commission on Critical Infrastructure Protection, October 1997, pg. 20, http://www.ciao.gov/PCCIP/PCCIP_Report.pdf (Link active as of 15 February 2002

Figure 4: Overview of the Cyber-Threat Spectrum

Figure 5, also taken from the "Technology Collection Trends in the U.S. Defense Industry" report covering the year 2000, breaks down the categories by which information requests originate. Note that, while the Internet represents only 2% of the recorded requests, it must be considered the primary "weapon of choice" in any future cyber-attack scenarios.

Table 21, "Technology Interest Trends" and Table 22, "Collection Incidents for Information Systems Subcategories per Year" provide further insight into the increasing interest by U.S. "adversaries" in critical infrastructure technologies, particularly those that provide potential opportunities for cyber-attacks. Table 21 is sorted, in decreasing order, by the number of collection incidents in 2000.

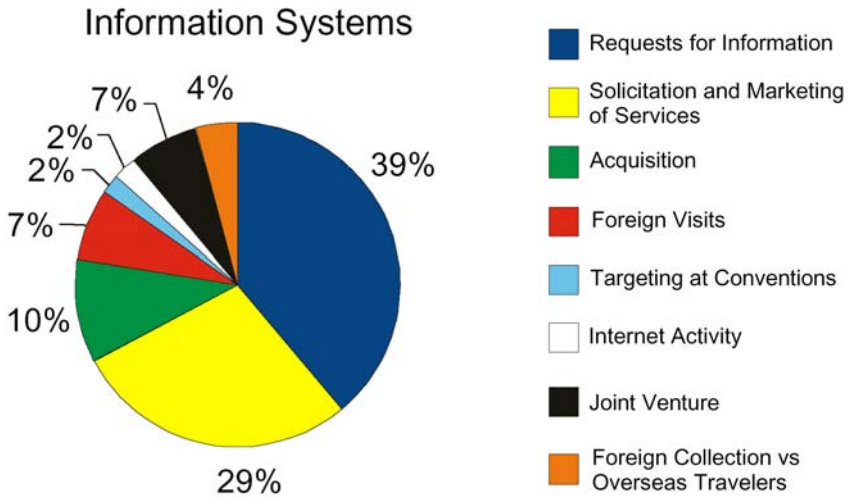


Figure taken from "Technology Collection Trends in the U.S. Defense Industry", U.S. Defense Security Service, Vol. VII, 2001, http://www.dss.mil/cithreats/2001_trend.pdf (Link active as of 8 February 2002)

Figure 5: Breakdown of Requests for Information Systems Data for the Year 2000

The President's Commission on Critical Infrastructure Protection identified five specific examples of new types of cyber-attacks to help illustrate the way that common software tools can be used to inflict harm. These include:

- **Cyber-attack on the specific database of an owner/operator**

  This category covers unauthorized entry into a network or system for the purpose of illegal financial transfers, stealing proprietary/classified

information, or merely browsing. Owners/operators have the responsibility to incorporate prudent security systems such as firewalls and passwords, as well as to employ qualified personnel to detect and recognize anomalies that indicate successful entry.

- **Cyber-attack for the purpose of gaining access to a network**

  If a system or network is discovered, through "electronic reconnaissance", to have low security standards, and it is also interconnected to other networks of interest to the attacker, then the most weakly defended pathway for access into the targeted system will be used. By transferal, owners/operators need to also be concerned about security standards for those with whom they are connected.

Table 21: Technology Interest Trends

Military Critical Technology List	Percentage Targeted
Information Systems	**30.0%**
Sensors and Lasers	**17.0%**
Aeronautics	**9.0%**
Armaments and Energetic Materials	**8.0%**
Electronics	**8.0%**
Marine Systems	**6.0%**
Chemical/Biological Systems	**3.0%**
Manufacturing and Fabrication	**3.0%**
Signature Control	**2.5%**
Guidance/Navigation/Vehicle	**2.5%**
Space Systems	**2.5%**
Materials	**2.0%**
Nuclear Systems Technology	**1.5%**
Ground Systems	**1.5%**
Information Warfare	**0.5%**
Power Systems	**0.5%**

Table 22: Collection Incidents for Information Subsystems by Year

Subcategory	1996	1997	1998	1999	2000
Software Systems	5	10	15	13	**33**
Transmission Systems	21	5	6	4	**29**
Information Security	7	13	6	2	**21**
Modeling and Simulation	5	5	6	6	**12**
Intelligence Systems	8	4	3	0	**11**
Signal Processing	2	0	1	3	**9**
Command, Control Communications, Computing, Intelligence (C^4I)	4	6	5	5	**8**
Computer-Aided Design (CAD)/Computer-Aided Manufacturing (CAM)	0	1	1	2	**4**
High-Performance Computing	5	2	5	0	**3**
Network Switching	0	4	1	0	**1**

- **Cyber-attack for the purpose of espionage**

  The vulnerability of intellectual property to theft may come from threats emanating from a witting or unwitting insider, an unscrupulous competitor, the intelligence service of a foreign power, or agents of a terrorist organization. Competitive advantage may be lost without even knowing that it was at risk.

- **Cyber-attack for the purpose of shutting down service**

  Attacks by flooding communication lines have denied 911 service in some communities and shut down e-mail service to major users. Denial-of-service attacks can be mitigated by sharing information about the tools used in these attacks, and the techniques that are successful in deflecting or defeating them.

- **Cyber-attack to introduce harmful instructions**

  Attackers can plant a virus, or embed a program that will provide them with critical information such as passwords that will allow access to other networks. Viruses can be transmitted within a Local Area Network (LAN) or passed on to an external net. It is essential that all interconnected users adopt, and keep current, a high level of virus detection.

Figure 6, from the "Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences" Report, provides insight into the potential damage that can be inflicted on systems that support the U.S. critical infrastructure by a variety of potential and real threats.

A survey of 2,545 information security practitioners, conducted by Information Security Magazine ("2001 Industry Survey", Information Security, October 2001, http://www.infosecuritymag.com/articles/october01/images/survey.pdf (Link active as of 8 March 2002)), illustrates the profile of internal and external security breaches experienced by the survey respondents for the year 2000 and 2001. These results are shown in Figure 7.

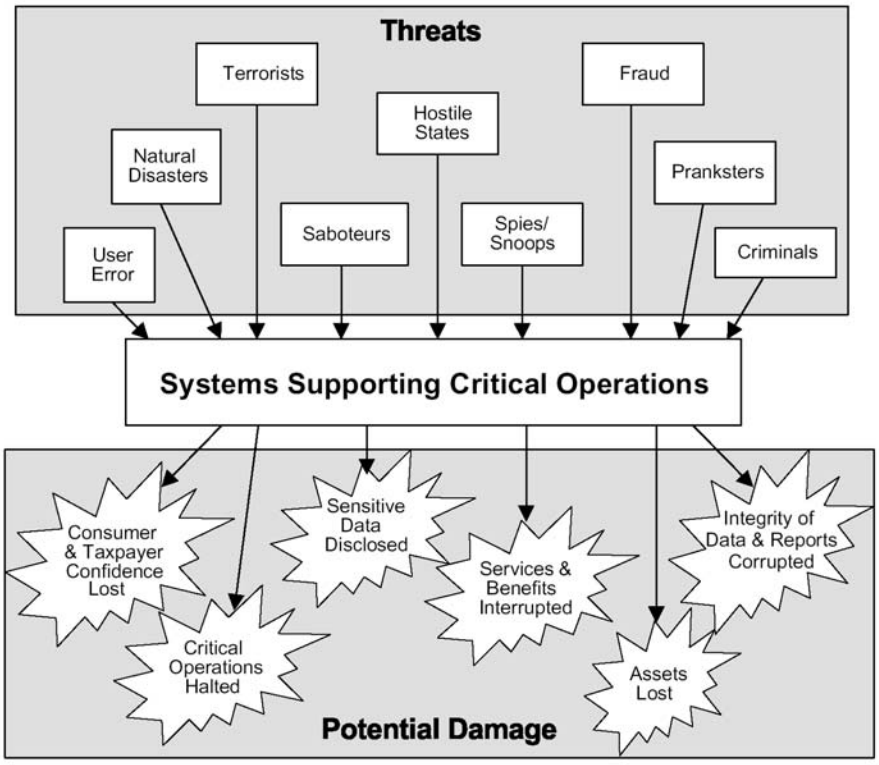
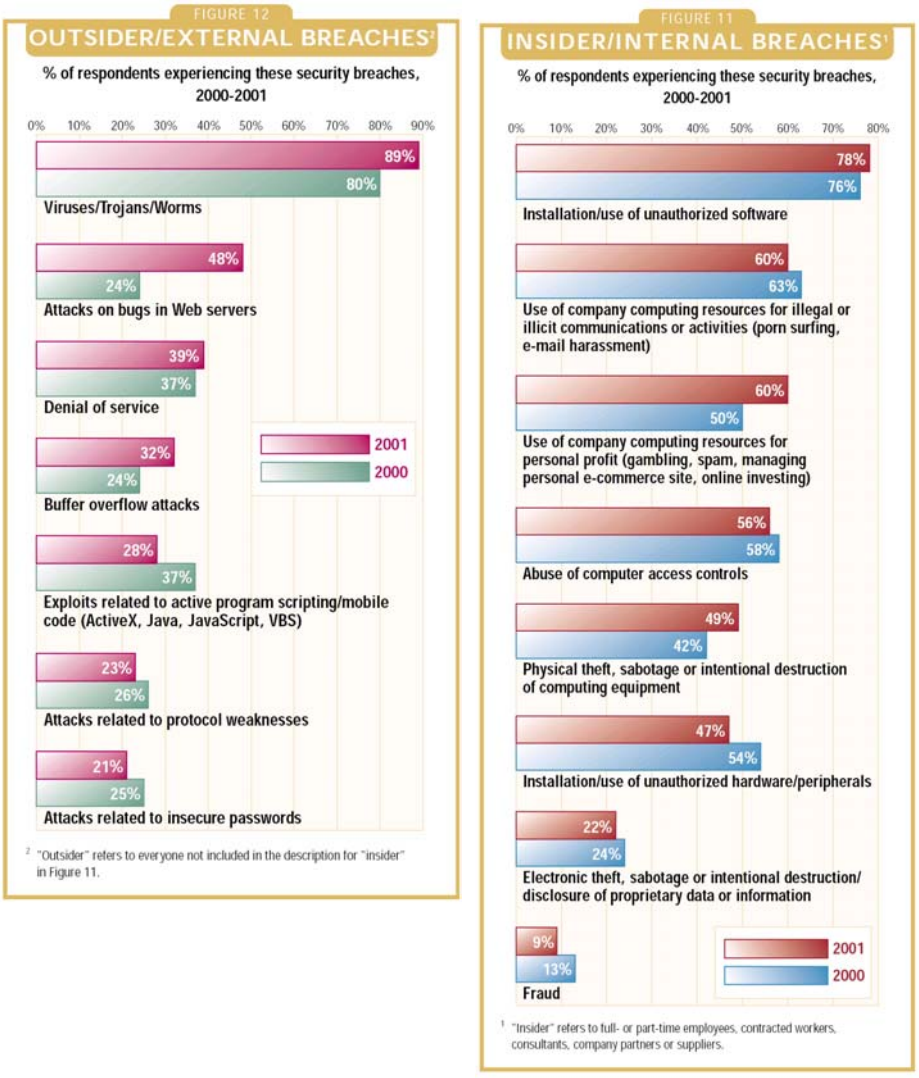


Figure 1 from "Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences"; Report to the Chairman, Special Committee on the Year 2000 Technology Problem, U.S. Senate; U.S. General Accounting Office Report GAO/ AIMD-00-1; October 1999;
http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00001.pdf&directory=/diskb/wais/data/gao

Figure 6: The Threats and Potential Damage to Systems That Support Critical Operations

For outsider/external breaches, survey respondents indicated an increase of approximately 10% in virus/trojan/worm attacks in 2001 over those in 2000. Attacks on web server bugs showed a dramatic 100% increase in activity, from 24% to 48%. Denial-of-service attacks had a modest increase of 5%, while buffer-overflow breaches rose by a third. Survey respondents reported slight decreases in attacks associated with exploits related to active program scripting/mobile code, attacks related to protocol weaknesses, and attacks related to insecure passwords. By far, the most active category for outsider/external breaches was viruses/trojans/worms, as reported by 80% of the respondents in 2000, and 89% in 2001.



Taken from "2001 Industry Survey", Information Security, October 2001, http://www.infosecuritymag.com/articles/october01/images/survey.pdf (Link active as of 8 March 2002

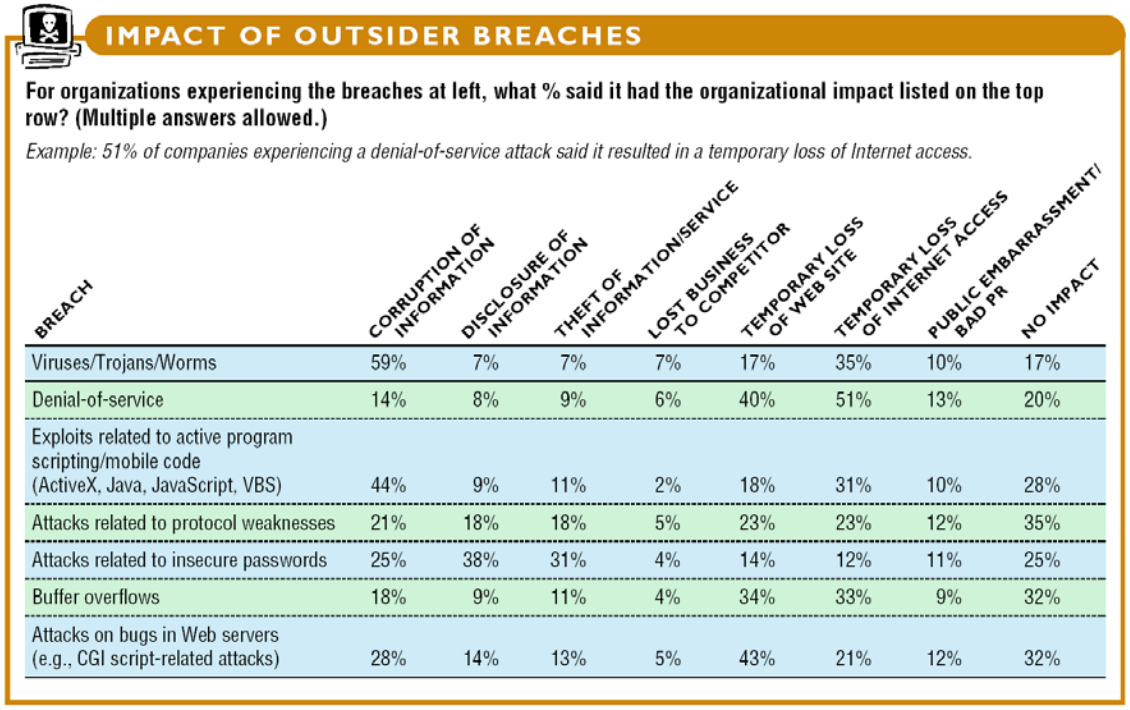
Figure 7: Comparison of Outsider/External and Insider/Internal Security Breaches (2000 vs. 2001)

For insider/internal breaches, there were relatively minor differences between 2000 and 2001 activity in the areas of installation/use of unauthorized software; use of company computer resources for illegal or illicit communications or activities; abuse of computer access controls; and electronic theft, sabotage, or intentional destruction/disclosure of proprietary data or information. Percentages of insider/internal breaches were registered by approximately 50% and higher of the respondents for 6 out of the 8 categories listed,

however, indicating the importance of not overlooking these types of activities as potential threats to critical infrastructure protection.

The potential impact on operations of both internal and external breaches is best summarized in Figures 8 and 9, taken from the 2000 Industry Survey conducted and published by Information Security magazine. Corruption of information and temporary loss of website or internet access are the predominant "casualties" of outsider/external attacks. For internal breaches, corruption, disclosure and/or theft of information represent the most likely outcomes.

The Vatis report, "Cyber Attacks During the War on Terrorism", having been issued shortly after the 9/11 attacks, provides a more detailed overview of the modes and mechanisms of cyber-threats and attacks. These are summarized in Table 23.



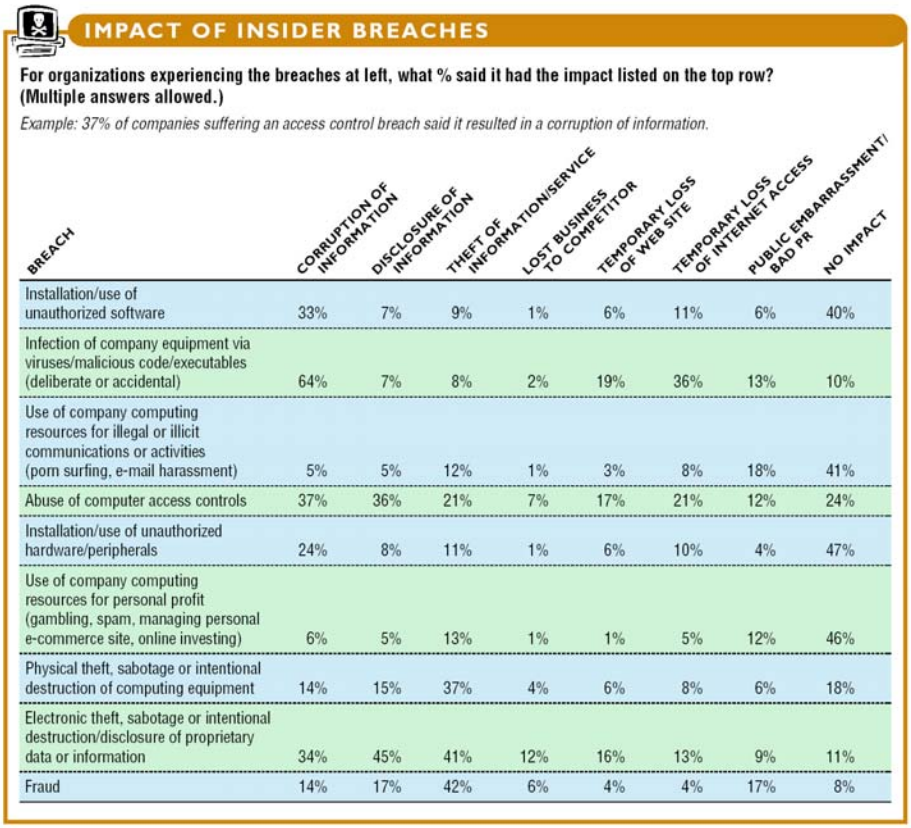
IMPACT OF OUTSIDER BREACHES

For organizations experiencing the breaches at left, what % said it had the organizational impact listed on the top row? (Multiple answers allowed.)

Example: 51% of companies experiencing a denial-of-service attack said it resulted in a temporary loss of Internet access.

BREACH	CORRUPTION OF INFORMATION	DISCLOSURE OF INFORMATION	THEFT OF INFORMATION/SERVICE	LOST BUSINESS TO COMPETITOR	TEMPORARY LOSS OF WEB SITE	TEMPORARY LOSS OF INTERNET ACCESS	PUBLIC EMBARRASSMENT/ BAD PR	NO IMPACT
Viruses/Trojans/Worms	59%	7%	7%	7%	17%	35%	10%	17%
Denial-of-service	14%	8%	9%	6%	40%	51%	13%	20%
Exploits related to active program scripting/mobile code (ActiveX, Java, JavaScript, VBS)	44%	9%	11%	2%	18%	31%	10%	28%
Attacks related to protocol weaknesses	21%	18%	18%	5%	23%	23%	12%	35%
Attacks related to insecure passwords	25%	38%	31%	4%	14%	12%	11%	25%
Buffer overflows	18%	9%	11%	4%	34%	33%	9%	32%
Attacks on bugs in Web servers (e.g., CGI script-related attacks)	28%	14%	13%	5%	43%	21%	12%	32%

Figure 8: Impact of Outsider Breaches (for 2000)



IMPACT OF INSIDER BREACHES

For organizations experiencing the breaches at left, what % said it had the impact listed on the top row? (Multiple answers allowed.)

Example: 37% of companies suffering an access control breach said it resulted in a corruption of information.

BREACH	CORRUPTION OF INFORMATION	DISCLOSURE OF INFORMATION	THEFT OF INFORMATION/SERVICE	LOST BUSINESS TO COMPETITOR	TEMPORARY LOSS OF WEB SITE	TEMPORARY LOSS OF INTERNET ACCESS	PUBLIC EMBARRASSMENT/ BAD PR	NO IMPACT
Installation/use of unauthorized software	33%	7%	9%	1%	6%	11%	6%	40%
Infection of company equipment via viruses/malicious code/executables (deliberate or accidental)	64%	7%	8%	2%	19%	36%	13%	10%
Use of company computing resources for illegal or illicit communications or activities (porn surfing, e-mail harassment)	5%	5%	12%	1%	3%	8%	18%	41%
Abuse of computer access controls	37%	36%	21%	7%	17%	21%	12%	24%
Installation/use of unauthorized hardware/peripherals	24%	8%	11%	1%	6%	10%	4%	47%
Use of company computing resources for personal profit (gambling, spam, managing personal e-commerce site, online investing)	6%	5%	13%	1%	1%	5%	12%	46%
Physical theft, sabotage or intentional destruction of computing equipment	14%	15%	37%	4%	6%	8%	6%	18%
Electronic theft, sabotage or intentional destruction/disclosure of proprietary data or information	34%	45%	41%	12%	16%	13%	9%	11%
Fraud	14%	17%	42%	6%	4%	4%	17%	8%

Figure 9: Impact of Insider Breaches (for 2000)

Table 23: The Modes and Mechanisms of Cyber-Threats

Lessons from Recent Cyber-Attack Case Studies	
• **Cyber-attacks immediately accompany physical attacks**	There is a direct relationship between political conflicts and increased cyber-attack activity. The resulting cyber-activity can have concrete political and economic consequences.
• **Cyber-attacks are increasing in volume, sophistication and coordination**	Approx. 1200 U.S. sites, including Government agencies, were subjected to cyber-attacks during one week in 2001, subsequent to the U.S./China spy plane incident. Recent cyber-attacks have also shown a pattern of phased escalation.
• **Cyber-attackers are attracted to high value targets**	Electronic high value targets are networks, servers or routers whose disruption would have symbolic, financial, political or tactical consequences.

Table 23: The Modes and Mechanisms of Cyber-Threats (continued)

Relevant Trends in Cyber-Attacks	
• **Worms**	The terms virus and worm are often used synonymously to describe malicious, autonomous computer programs. Recent worms (Code Red, Code Red II, Nimda) have become progressively more sophisticated, each enhancing the attack capabilities of its predecessor.
• **Distributed Denial-of-Service (DDoS)**	Employ armies of "zombie" machines taken over and controlled by a single master to overwhelm the resources of victims with floods of packets.
• **Unauthorized Intrusions**	Theft of money or credit card numbers, proprietary information, or sensitive Government information can have devastating consequences.
Potential Sources of Cyber-Attacks	
• **Terrorist groups**	Terrorists are known to be extensively using information technology and the Internet to formulate plans, raise funds, spread propaganda and communicate securely.
• **Targeted nation-states**	Many foreign nations have identified the utility of developing cyber-attack techniques for purposes of engaging in covert espionage. Nations thought to be developing information warfare capabilities include Iraq, Libya, China, North Korea, Cuba and Russia.
• **Terrorist sympathizers and anti-U.S. hackers**	Attacks by those sympathetic to terrorist group(s), or with general anti-U.S. and anti-allied sentiments, may become more likely than those by terrorists themselves, or by nation-states.
• **Thrill seekers**	This category of hackers may not be driven by political ideology, but by the desire to gain personal notoriety through their exploits.
Cyber-Attackers During the War on Terrorism are Likely to Use:	
• **Web defacements and semantic attacks**	Politically motivated website defacements will likely escalate. These can include explicit propaganda, or more sinister "semantic" attacks that involve subtle content changes that disseminate false information.
• **Domain Name Service (DNS) attacks**	If DNS servers are provided an incorrect numerical address, the user could be connected to a counterfeit connection without arousing suspicion.
• **Denial-of-Service (DoS) attacks**	Attacks against high value targets are expected to increase, with potential coordinated attacks considered particularly dangerous.
• **Worms**	An unprecedented number of prolific worms (e.g., Code Red, Ramen, Lion), some of which may have been inspired by political events. New classes of faster, more ominous worms (Warhol worms, flash worms), as well as hybrid worms, may soon emerge.

Table 23: The Modes and Mechanisms of Cyber-Threats (continued)

Cyber-Attackers During the War on Terrorism are Likely to Use (continued):	
• **Routing vulnerabilities**	Lack of diversity in router operating systems leaves open the possibility of massive router attack. A lack of cyber-diversity (i.e., the reliance on a single hardware or software product for certain functions) increases the chances of a simplistic, but highly effective, cyber-attack.
• **Unauthorized intrusions into systems and networks**	Cyber-attacks against infrastructures using unauthorized intrusions, DDoS attacks, worms, Trojan horse programs, or malicious insiders may be used to exploit current or future vulnerabilities.
• **Compound attacks**	Individually, any one of the above scenarios could have serious consequences. A multi-pronged attack employing some or all of these scenarios could be devastating to whoever is unprepared.
Critical Cyber-Security Measures During the War on Terrorism:	
• **Raise/maintain heightened cyber-alert and logging levels**	System administrators and Government officials should be on high alert for cyber-attack warning signs, particularly following military strikes or covert operations. Changes in "normal" scanning activity should be considered highly suspicious. Logging levels should be temporarily raised to trap as many events as possible to increase the fidelity of subsequent law enforcement or counterintelligence investigations, and enable specific warnings by the NIPC.
• **Report suspicious activity to law enforcement**	Law enforcement contact numbers should be readily available in case of a cyber-attack.
• **Apply/follow standard security "best practices"**	Best practices for maintaining systems should be followed as part of normal operating procedures: • Operating systems and software should be updated regularly • Strong password policies should be enforced • Systems should be "locked down" • All unnecessary services should be disabled • Anti-virus software should be installed and kept current • High fidelity intrusion detection systems (IDS) and firewalls should be used Security measures which, in the past, may have been considered excessive should now be considered as minimum requirements.

Table 23: The Modes and Mechanisms of Cyber-Threats (continued)

Critical Cyber-Security Measures During the War on Terrorism (continued):	
• **Secure critical information assets**	A critical information asset is any host or network whose loss might result in serious communications failure or financial impact. Steps that should be taken include: • Use of anti-defacement measures that include checks for common defacement characters • Border routers that use existing authentication mechanisms to prevent malicious tampering • Domain name servers running only recent/secure software to prevent DNS corruption and redirection of web traffic • Regular backup of all vital data, stored off-site • Copy/maintain log records in a secure location to avoid tampering • Explanation of all measures to secure critical information assets in an enforceable security policy
• **Use ingress/egress filtering to protect against DDoS attacks**	"Spoofed" Internet Protocol (IP) addresses are easy to detect and stop at their source, since routers can be programmed to discard any outbound packets whose source IP address does not belong to the router's client networks (egress filtering). Inbound (or ingress) filtering of any IP packets with untrusted source addresses (e.g., those addresses reserved for private networks or not yet issued by international authorities) before they enter a network can also be effective.

In his 29 August 2001 testimony before the House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Stephen Trilling (Senior Director of Advanced Concepts – Symantec Corporation) outlined several top security recommendations for any public or private organization that may protect against up to 80 percent of cyber-attacks:

- Organizations need properly configured and regularly updated antivirus software and firewalls as a basis for effective security
- Organizations need to deploy appropriate updates for any announced security holes, on all systems, as soon as they become available
- Organizations should have a specific policy to ensure that computer users' passwords cannot easily be compromised
- Organizations should take more proactive steps to deploy vulnerability assessment and management software

- Organizations should consider blocking all executable programs flowing into the corporation through e-mail attachments
- Organizations should consider installing intrusion detection software to monitor their networks for potential attacks
- Organizations should deploy several layers of security software at all tiers within the enterprise
- Industries and Government agencies that are essential to national security should consider using private networks for all critical communications
- There is a need to continue private/public sector cooperation in sharing information on security issues, as well as providing appropriate security education to both Government and corporate entities

7.3 DoD Critical Infrastructure Protection

As "far back" as May 1996, the DoD was cognizant of the major elements of critical infrastructure protection that all of the security studies and experts agreed were important, as published in their "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" Report to Congressional Requestors (GAO/AIMD-96-84):

- Clear and consistent information security policies and procedures
- Vulnerability assessments to identify security weaknesses at individual Defense installations
- Mandatory correction of identified network/system security weaknesses
- Mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions
- Damage assessments to re-establish the integrity of the information compromised by an attacker
- Awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security
- Assurance that network managers and system administrators have sufficient time and training to do their jobs

- Prudent use of firewalls, smart cards and other technical solutions
- An incident response capability to aggressively detect and react to attacks, and track and prosecute attackers

Y2K computer systems conversion and critical information system protection share a need to rapidly develop a national capability to reconstitute critical cyber-systems that fail. Y2K planners prepared for critical infrastructure systems that may have failed or been attacked during the rollover events. A national system of joint Federal-private sector resources was created in order to monitor, coordinate and assist, if necessary, in the reconstitution of vital cyber-systems during the Y2K rollover

On 18 November 1998, and in response to PDD 63, the DoD released its 104-page "The Department of Defense Critical Infrastructure Protection (CIP) Plan" to address how the DoD would protect its portion of the Federal Government Critical Infrastructure. The DoD portion was defined as (1) Defense Financial Services, (2) the Defense Information Infrastructure, (3) Defense Logistics, (4) Defense Transportation, (5) Defense Space, (6) Defense Personnel, (7) Defense Health Affairs, (8) Defense Public Works, (9) Defense Command, Control and Communications, (10) Defense Intelligence, Surveillance and Reconnaissance, and (11) Defense Emergency Preparedness.

The portion of the national infrastructure that directly supports the Defense Infrastructure is defined as the National Defense Infrastructure. As the CIP Functional Coordinator for National Defense, DoD is responsible for identifying the National Defense Infrastructure and working jointly with the national CIP organizational structure and the private sector to ensure its protection.

The DoD Critical Infrastructure Protection Program is intended to address the full life cycle of protection, with the life cycle phases being defined as:

- **Infrastructure Analysis and Assessment:** Coordinated identification of DoD, National Defense, and International Defense critical assets, their system and infrastructure configuration and characteristics, and the interrelationships among

infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets/infrastructures; and assessment of the operational impact of infrastructure loss or compromise

- **Remediation:** Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc., of critical assets and infrastructure, e.g., emergency planning for load shedding, graceful degradation and priority restoration; increased awareness, training and education; changes in business practices or operating procedures, asset hardening or design improvements, and system-level changes such as physical diversity, deception, redundancy and backups

- **Indications and Warning:** Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the National Infrastructure Protection Center in concert with existing DoD and national capabilities

- **Mitigation:** Pre-planned and coordinated operator reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigation, and crisis management response; and facilitate reconstitution

- **Response:** Coordinated third party (not owner/operator) emergency, law enforcement, investigation, defense, or other crisis management services aimed at the source or cause of the incident

- **Reconstitution:** Owner/operator-directed restoration of critical assets and infrastructure

As documented in the "Report of the President of the United States on the Status of Federal Critical Information Structure Initiatives", January 2001, the Department of Defense defined its Critical Infrastructure Protection vision as "an integrated, warfighter-focused effort to identify and mitigate vulnerabilities of critical assets to commander-in-chief (CINC) mission accomplishment and operational readiness." The CIP vision establishes and maintains a comprehensive, fully integrated and sustainable cyber and physical program for ensuring the availability of infrastructures critical to national security. The vision looks at what is needed to meet the defense mission (e.g., facilities, equipment, information systems, communication systems/networks, people, power, contracts, etc.), then determines what are the most critical assets, identifies their

associated vulnerabilities, recognizes infrastructure interdependencies. Measures are then taken to reduce those vulnerabilities.

Incorporated into the DoD CIP implementation plan are unique sets of functions, including military plans and operations; international cooperation; intelligence support; research and development; and education and awareness. For each of these functions, lead Components within the DoD have been designated to integrate the national defense activities across the various sectors and the other functions at the national level. The DoD plan calls for, and the Department has established, a staff responsible for integrating and coordinating all CIP activities for the Department.

Figure 10 and Table 24 represent a high-level overview of the DoD's organizational structure for Critical Infrastructure Protection.

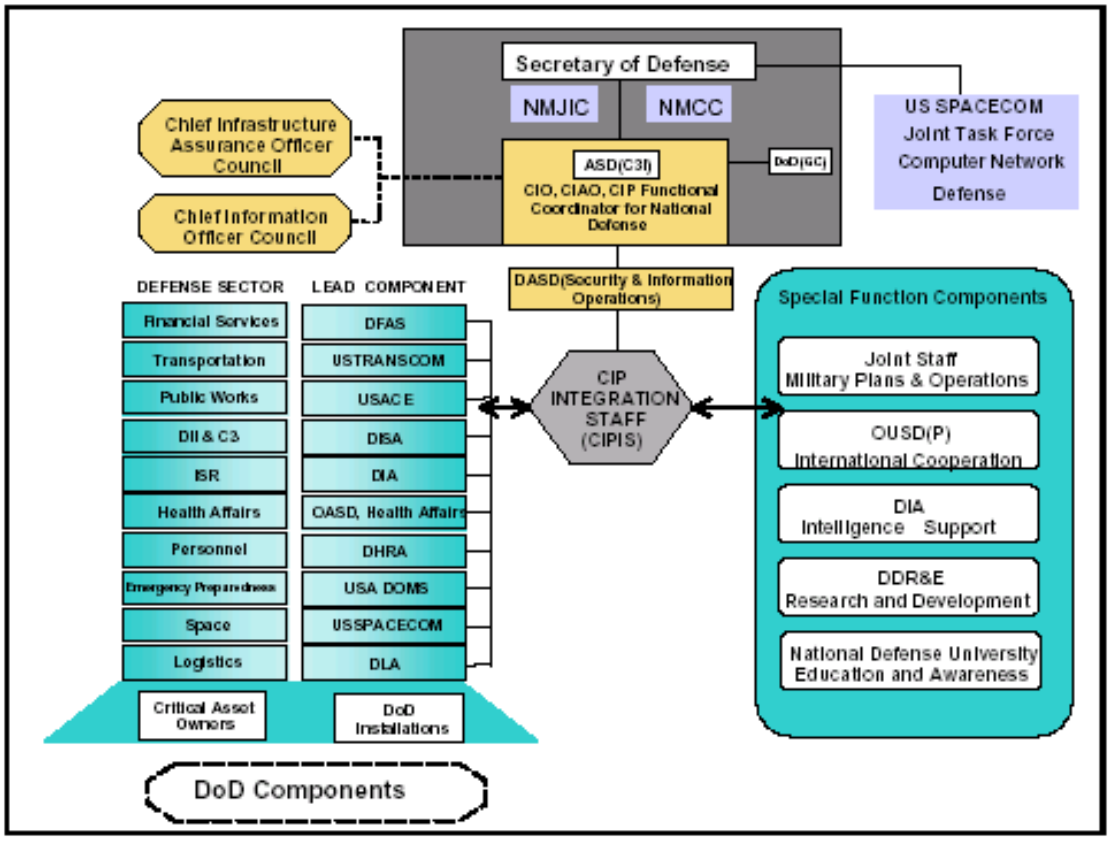


Figure 10: DoD Structure for Critical Infrastructure Protection

Table 24: DoD Defense Sectors and Lead Components

Defense Infrastructure Sector	Lead Component for Sector Assurance Coordination
Defense Information Infrastructure Command, Control & Communications (C^3I)	Defense Information Systems Agency (DISA)
Emergency Preparedness	U.S. Army, Director of Military Support
Financial Services	Defense Finance and Accounting Service
Health Affairs	OASD, Health Affairs
Intelligence, Surveillance and Reconnaissance	Defense Intelligence Agency (DIA)
Logistics	Defense Logistics Agency (DLA)
Personnel	Defense Human Resources Agency
Public Works	U.S. Army Corps of Engineers
Space	U.S. Space Command
Transportation	U.S. Transportation Command

7.4 Lessons Learned

The "Critical Foundations: Protecting America's Infrastructure" report mentioned previously, even though it preceded the Y2K rollover event, proposed many of the principles for protecting our critical infrastructures that would ultimately prove to be successful in meeting the Y2K challenge.

- ***Build on that which exists.*** Countermeasures will be easier and faster to implement, more effective, and more likely to be accepted than creating something new.

- ***Depend on voluntary cooperation.*** Partnerships between industry and Government will be more effective than legislation or regulation.

- ***Start with the owners and operators.*** They have a strong economic stake in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and have experience in responding to outages.

- ***Practice continuous improvement.*** Take action in affordable increments, recognizing that there will be no "silver bullet" solution. Aim to enhance, as well as protect, the infrastructures.

- ***Coordinate security with maintenance and upgrades.*** Security should be incorporated in planned maintenance and scheduled upgrades.

- ***Promote Governmental leadership by example.*** Government-owned facilities should be the first to adopt best practices, active risk management and improved security planning.

- ***Minimize changes to Government oversight and regulation.*** Several critical infrastructures have a long history of Government regulation, with a clear legislative mandate and record of success. Significant changes in regulation should be avoided.

The Final Committee Report of the U.S. Senate Special Committee on the Year 2000 Technology Problem entitled "Y2K Aftermath – Crisis Averted" pondered ways in which the Y2K experience could be leveraged to benefit future high-tech infrastructure protection, recognizing that improving critical infrastructure protection was the next major challenge to the IT community. Suggestions/recommendations made within the report included:

> **Maintain/Enhance Y2K Networks and Public/Private Partnerships:** The public/private relationships established during the Y2K effort will prove invaluable for future IT efforts. The challenge of protecting critical infrastructures from computer-based attacks extends well beyond Federal operations, spanning the entire spectrum of the national and global economies. Public/private partnerships are recognized as one of the major challenges of critical infrastructure protection, particularly in view of their vast interdependencies and shared vulnerabilities.
>
> **Leverage Y2K Lessons to Improve Infrastructure Protection:** The preparation for Y2K prompted a significant worldwide investment in business information systems and high-tech infrastructures. This rapid increase in globalization has associated risks. Interconnectivity and public access to U.S. information systems increases its vulnerability to cyber-attacks. A significant challenge to U.S. policymakers lies in devising methods to detect, deter and respond to information attacks against critical infrastructures.

As previously mentioned, lessons learned from the Y2K conversion effort are relevant to public-private partnerships for information security. Incorporating this information dimension into service and product delivery assurance programs requires that each organization:

- assess dependency of critical operations on information technology
- review impact and consequences to business operations and customer relationships when information flow is disrupted or corrupted from intentional or accidental acts

- evaluate change in risk profiles and take remedial action as required by prudent management and due diligence to ensure delivery of services or products that meet customer and public expectations

- continue to appraise future information technology investments to include security risks to critical business operations

In 27 January 2000 testimony before the House Subcommittee on Government Management, Information, and Technology and the House Subcommittee on Technology, then-CIO for the Department of State, Fernando Burbano, identified a number of Y2K lessons learned and legacy products and processes that could be leveraged directly into Critical Infrastructure Protection planning, management and execution. These are highlighted in Table 25 and briefly discussed below.

Table 25: Y2K Lessons Learned Reuse Assessment

Reuse Item	PDD-63	CIP Initiatives	Clinger-Cohen	GPRA
Separate supplemental funding	**F**	**F**	**-**	**-**
Senior-level sponsorship	**F**	**F**	**F**	**F**
Repeatable and measurable metrics	**F**	**F**	**F**	**P**
IT product inventory	**M**	**M**	**F**	**P**
Contingency plan development	**F**	**F**	**-**	**-**
Global reporting	**M**	**M**	**P**	**P**
Public/private cooperation	**F**	**F**	**M**	**P**

LEGEND: **F (Full)** - Reuse item can be fully leveraged into the Federal initiative
M (Most) - With some minor modification, the Reuse item can be leveraged into the Federal initiative
P (Partial) - Some aspects of the Reuse item can be leveraged into the Federal initiative

During Y2K, ***separate supplemental funding***, in addition to basic core funding, was provided to agencies to support implementation of remediation and preparation efforts. The majority of CIOs across the Federal Government believe that without this supplemental funding, their Y2K efforts would have been unsuccessful.

Buy-in and leadership from ***senior level sponsors*** within the Federal Government and individual agencies, including agency Secretaries, Under Secretaries and Assistant Secretaries, placed the responsibility and accountability of product tasks, activities and milestones at levels that could quickly effect change and acquire necessary resources. Emphasis on the importance of addressing the Y2K problem trickled down through each organization and provided the Y2K programs with effectively staffed remediation teams.

Repeatable and measurable project and performance ***metrics*** at both the agency- and Federal-level gave Y2K Project Managers the ability to assess current status and progress against Federal milestones. The Government-wide management approaches which incorporated these metrics included Executive and Congressional oversight and agency-level performance across a variety of areas (e.g., project cost, technical issues, risk management and schedule). This same management structure and discipline, including Assistant Secretary-level management and repeatable standardized measures and processes, can, and should, also be applied to Critical Infrastructure Protection.

A detailed ***IT product inventory*** of each agency's mission-essential systems and information technology was thoroughly disseminated, tested at a system level, independently verified and placed under strict enterprise-wide configuration control. Most agency Y2K preparations began with the development of a complete, prioritized list of the organization's IT applications. This IT inventory was a critical first step to identifying and refining the mission-essential infrastructure of an agency as required by PDD-63.

Mission-based ***contingency plans*** of all critical business processes were developed and tested by all elements of the Federal Government. The development of these contingency plans resulted in a greater understanding of the dependency of business processes on IT systems by senior policy managers. In addition, these plans are "durable" beyond Y2K and can establish the foundation for all future contingency operations planning.

For the Y2K rollover period, the Government developed a robust ***global reporting*** structure that captured specific Y2K status, in real-time, of vital domestic and international concerns within central data coordination centers. This same structure can be leveraged into a mechanism for monitoring and communicating cyber-threats against critical infrastructure elements.

Barbano's testimony again reinforced the fact that a major component of Y2K success was the unprecedented level of ***public/private cooperation*** and coordination between Government agencies and private industry. In many instances, Federal project managers were rapidly able to gain access to business-sensitive or proprietary tools and techniques. Federal agencies were able to obtain information and identify subject matter experts in a variety of Y2K-related areas without the need to navigate through typical bureaucratic obstacles. Additionally, Congressional support in areas such as minimizing potential Y2K litigation through Good Samaritan legislation provided the private sector with enough legal protection that they could be open to share new ideas without the usual warranty ramifications.

As a result of developing the products and instituting the processes for Y2K, the Government has seemingly accelerated the process of implementing Critical Infrastructure Protection programs.

In his book, "Y2K Lessons Learned: A Guide to Better Information Technology Management", Timothy Braithwaite provides a set of recommendations on what lessons can/should be learned from Y2K as they apply to higher-level IT project and process management. Although discussed mostly in the context of the private sector, it is not difficult to see how these recommendations can be leveraged to address critical infrastructure protection solutions. Table 26 highlights these recommendations.

Table 26: Recommendations for Successful IT Management Based on Y2K Lessons Learned (Derived from Braithwaite)

Lesson Learned	Recommendations
Establish Executive Ownership of Information and IT Projects	Recommendation 1: Establish or reinvigorate the executive IT committee chaired by the Chief Executive Officer Recommendation 2: Based on current inventory data, ensure that all automated business systems, software application systems, and processing support systems are the direct responsibility of some member of the executive IT management committee

Table 26: Recommendations for Successful IT Management Based on Y2K Lessons Learned (Derived from Braithwaite) (continued)

Lesson Learned	Recommendations
Determine Appropriateness of IT Projects Through Expanded Feasibility Analysis	Recommendation 3: Establish policy that all IT proposals be subjected to a full feasibility analysis conducted in the sequence of technical, operational, and economic studies Recommendation 4: Require that return on investment and cost ownership studies not be substituted for the economic study of the full feasibility analysis
Establish an Executive-Level IT Risk Management Review Process	Recommendation 5: Establish a practice that all corporate IT systems in current operation or under development; processing environments and support infrastructures (in-house or outsourced); and new contemplated technologies be assessed and continuously monitored for potential adverse impacts on the business. Reports should be presented periodically to the executive IT management activity.
Make Improvements to IT Management	The most critical improvements that can be made in support of effective IT management are those that require and enforce forms of personal and organizational accountability
Require Development and Delivery Methodologies	Recommendation 6: Establish a policy that all corporate system and software developments and integration efforts are to be guided by a systems development process or methodology that incorporates the life-cycle phases of preparation, definition, design, development, deployment and maintenance, or the equivalent. Enforce its use. Recommendation 7: The Executive IT Management Committee should commission an evaluation of current corporate software development and maintenance capabilities using the SEI's capability maturity model (CMM) Recommendation 8: In order to progress beyond SEI Level 1, establish a software development and systems management metrics program and begin building the databases of experiential data upon which higher levels of the CMM can be built
Customer Relations and Technical Support	Recommendation 9: Executive members of the IT management committee need to re-dedicate themselves, the IT group, support contractors, and suppliers to the practices of quality management and continuous process improvement. Promotion and reward systems need to be aligned with this emphasis. Executive management must act as final arbiter when there are conflicts among quality, expediency, and the customer.
IT Vendor and Supplier Selection	Recommendation 10: Establish IT process management criteria for selecting future vendors and suppliers. Include the capability maturity model evaluation method, independent verification and testing of products, and performance benchmarking. Establish selection evaluation committees with membership that represents all stakeholders to every project.

Table 26: Recommendations for Successful IT Management Based on Y2K Lessons Learned (Derived from Braithwaite) (continued)

Lesson Learned	Recommendations
Outsourcing IT Support	Recommendation 11: Commission a review of all existing and pending company outsource arrangements to identify any risky dependencies or vulnerabilities that could threaten the viability of the corporation. For pending outsource arrangements, require that a comprehensive feasibility analysis be performed to allow for intelligent bidding, evaluation and contracting. Recommendation 12: Review all existing and pending outsource projects and plans to ensure adequacy of employee numbers and skills sufficient to monitor and manage the outsourcer.
IT Personnel Management	Recommendation 13: Commission an analysis of current human resource policies to determine their effectiveness regarding IT employees. Concentrate the review on those human resource practices needed to recruit, hire, train, compensate, utilize, and promote a workforce that will grow in company loyalty. Recommendation 14: Consider the creation of a core of IT employees to protect the company from the risks of outsourcing and contractor dependence. Design the core around those IT functions that must be preserved to guarantee continued corporate operations regardless of outsourcing contractor performance. Recommendation 15: Consider the creation of a technology and continuous improvement center chartered with innovating and improving the company's system products, services, and work processes. Treat the center as an overhead activity staffed, on a rotating basis, by IT employees and appropriate business unit employees.
Establishing IT Management Basics – A Period of Retrenchment	Recommendation 16: Commission a lessons-learned assessment of the corporation's Y2K experience, identifying those IT management processes that were deficient. Plan an orderly return-to-basics initiative to bring IT processes to the level of industry "best practices".

7.5 Lessons Perhaps Not Learned?

The May 2001 report "Year 2000 Lessons Learned: Strategies for Successful Global Project Management" issued by the Office of the Inspector General, U.S. Department of State, contained a lead-in quote which perhaps best summarizes why the lessons learned as part of the global Y2K effort are not being learned as quickly as they should/could be in addressing critical infrastructure issues:

> "*Y2K was fascinating in terms of how to get one's arms around a subtle problem that crossed a wide sweep: 180 countries, 50 states, the entire U.S. economy, and the whole U.S. Government.* ***We will not have to do it again in the near future (emphasis added)****, however the lessons learned from the exercise will be invaluable in addressing other management issues."*
>
> Chair, President's Council on Year 2000 Conversion, United States

The events of September 11th, and the increasing (and, some would say, long overdue) awareness of critical infrastructure vulnerabilities that have been highlighted by recent cyber-attacks poignantly emphasize the fact that "the future is now".

In a paper entitled "Overblown or Extremely Well Managed? – Solving Year 2000", Robert Parker makes a number of observations that indicate that the best practices and lessons learned from the Y2K effort are rapidly falling by the wayside:

> *"Already we have seen that entities that developed extensive asset management inventories, as well as clean and change management procedures, are letting these procedures fall by the wayside because of maintenance costs, lack of resources and other corporate priorities. Business continuity and disaster recovery plans are starting to gather dust. A planned and coordinated testing process has not been planned for the future.*
>
> *In short, we are at risk of losing many of the gains of the Year 2000. We are at risk of losing many of the best practices developed during Year 2000 preparation. We are at risk of not taking advantage of opportunities from the Year 2000 project."*

Parker explains that the responsibility for capturing these value-added best practices has fallen to the project management office, but these offices are (were) rapidly being downsized and dismantled, with the knowledge base quickly eroding as those with relevant expertise migrate to other tasks and business units. He identified several key factors that were inhibiting industry from continuing Y2K value-added best practices:

- Lack of funding
- Need not perceived
- Benefits not perceived or not sufficient to justify the costs
- Not supported by the corporate culture

- Lack of Year 2000 horror stories to convince organizations of the benefits and risks
- Concern that Year 2000 had already cost too much
- "On to the next project" syndrome (i.e., move resources to e-business and forget about the year 2000)

Almost 20% of the respondents to an Information Systems Audit and Control Association® (ISACA™) survey indicated that they would discontinue their business continuity objectives, with the most frequently cited reasons being lack of support, lack of funding, and benefits not perceived. Almost 20% of the survey respondents indicated that their quality assurance procedures would not be maintained, and 10% indicated that test strategies would not be continued. While these percentages may or may not seem alarming, there is a potentially high level of risk associated with having your organization dependent on these organizations when it comes to critical infrastructure protection, given the interdependencies between organizations and networks.

Following the successful completion of the Y2K rollover, many key voices were heard, and unheeded, in support of preserving the White House Y2K Information Coordination Center as a national defense facility against cyber-terrorism and other high-tech threats:

1. In February 2000, Sen. Robert Bennett stated that:

   "The national command center…was very effective…as a focal point for gathering and analyzing real-time information from around the world. The capabilities of this facility would be well-suited to dealing with the Information Age threats of hackers, cyber-terrorism, cyber-crime and information warfare."

2. In a June 2000 article in the American Society of Civil Engineers (ASCE) "Journal of Infrastructure Systems", Dr. William J. Harris observed that:

   "Y2K was a special case of cyber-security. A concentrated and coordinated effort eliminated programming and hardware problems and made the transition occur with very few glitches. However, shortly after Y2K, a series of successful denial-of-service attacks were made on many cyber-systems, which demonstrated their individual and collective vulnerabilities. Meanwhile, the engineering profession appears to have ignored this issue for the most part….The ***engineering professional societies have not focused attention on the role of the engineering***

profession with respect to cyber-security. Thus, we are confronting a challenge that will place enormous demands on the profession before it is resolved, but ***the engineering community has not yet established a unifying concept to characterize its role in addressing cyber-security***."

3. In July 2000, Ret. Lt. Gen. Peter Kind, the former Director of the Year 2000 Information Coordination Center, suggested that the Government missed a "golden opportunity" to mirror the lessons learned when it decided to dismantle the center rather than use it as a model for other joint systems efforts such as critical infrastructure protection. Earlier in 2000, some lawmakers and the companies that had provided equipment to the center suggested that OMB should use the center as a security facility to deal with systems attacks, but the OMB decided to stick with its original plan of distributing most of the systems and communications equipment to FEMA.

4. In August 2000, the president of the Information Technology Association of America (ITAA) proposed that the Government create an International Information Security Coordination Center modeled after the Year 2000 International Coordination Center. Harris N. Miller, president of the Association, was impressed that "the Y2K center was a lean and mean organization (that was) effective in coordinating both from the Government and the private sector side of the globe." For a security effort, this type of undertaking was recognized as being more challenging to keep focused, given that systems security problems comprise multiple issues, without the must-meet deadlines that characterized Y2K efforts. In October 2001, he commented that, while there was now a push on to recreate a Y2K-like command center to combat terrorist threats, the Y2K network should never have been shut down to begin with. "That was a decision made by the outgoing administration over our strong objections."

5. In November 2001, in an interview with National Journal's Technology Daily, Microsoft Chief Security Officer Howard Schmidt echoed the call for the rebirth of the Year 2000 Information Coordination Center in order to help companies susceptible to cyber-attacks. He indicated that "while many of the nation's largest companies have boosted their computer security to deter cyber-attacks, small and medium-sized companies remain the most vulnerable to malicious invasions." Reviving the center has been seen by many as a viable option for coordinating and disseminating early warnings regarding cyber-attacks. Schmidt also indicated that the Government expects to release a guideline for all businesses that will detail where to report computer attacks. The FBI and the private sector are also generating a checklist for businesses.

In testimony before the Subcommittee on Government Management, Information and Technology (26 July 2000), John Pescatore, VP and Research Director, Network Security, Gartner Group, Inc., observed that "while it was business as usual during the Year 2000 rollover period for most private industry computer systems, many Government

(both civilian and DoD) computer systems were shut down or disconnected from the Internet to avoid security problems. During the recent I Love You (ILU) virus attack, threat information seemed to flow much more slowly through Government reporting mechanisms than in private industry….The Government can also take heed of lessons learned during Y2K preparations and use mechanisms (such as the National Security Telecommunications Advisory Council) as models for how to spur sharing of security incident information….The Government can also learn from private industry, where industry groups such as Acord (the insurance industry), BITS (in the banking industry), the Forum of Incident Response Teams, and best practice groups such as those run by the Gartner Group provide rich mechanisms for industry to share security information."

Testimony by John Spotila, Administrator, Office of Information and Regulatory Affairs, on 11 September 2000 before the House Subcommittee on Government Management, Information and Technology noted several deficiencies that needed to be addressed in order to provide greater protection to the critical infrastructure:

- More agencies need to install firewalls at external entry points to exclude unauthorized users, and within their networks to ensure that authorized users do not exceed authorization
- Increased use of encryption by agencies would help promote confidentiality of sensitive material, such as password files and personal information
- Agencies need to improve their intrusion detection capabilities and procedures (including increased involvement of agency Privacy Officers and legal counsel in reviewing the monitoring activities)
- More agencies need to ensure that management authorizes system use consistent with security precautions
- More agencies must have independent reviews of their security plans

Similarly, in a September 2000 report (GAO/AIMD-00-295) to the Chairman of the House Subcommittee on Government Management, Information and Technology, entitled "Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies", it was stated that significant information security weaknesses remain

pervasive in each of the 24 agencies covered by the Committee analysis. A summary of these weaknesses circa September 2000 is illustrated in Table 27.

Table 27: Areas of Information Security Weakness for 24 Federal Agencies

General Control Area	Number of Agencies					
	Significant Weakness Identified		No Significant Weakness Identified		Area Not Reviewed	
	1998	2000	1998	2000	1998	2000
Access controls	23	24	0	0	1	0
Application software development and change controls	14	19	4	2	6	3
Entity-wide security program planning and management	17	21	0	0	7	3
Segregation of duties	16	17	1	3	7	4
Service continuity controls	20	20	0	1	4	3
System software controls	9	18	0	0	15	6

One year prior to this report, in August 1999, this same Subcommittee had reported specific, pervasive information security weaknesses within the DoD that could "seriously jeopardize operations and compromise the confidentiality, integrity or availability of sensitive information". These weaknesses continued to provide both hackers and a multitude of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DoD data, and impaired DoD's ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its systems was properly authorized, tested, and functioning as intended, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous DoD functions (including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll) had already been adversely affected by system attacks and fraud. While some progress had been made since August 1999, it was inconsistent across the various DoD Components. A May 2000 review by this committee of the DoD's financial management systems showed that serious weaknesses in access controls and system software still remained. The committee was able to exploit weaknesses to obtain sensitive information through a publicly available Internet file and, without valid user authentication, gained access to employees' social security numbers, addresses and pay information, as well as budget, expenditure and procurement information on projects. It was noted that DoD had been taking steps to improve its information security. Notably, the department had established

(1) the Defense-Wide Information Assurance Program under jurisdiction of the DoD CIO, and (2) the Joint Task Force for Computer Network Defense to monitor DoD computer networks and defend against hacker attacks and other unauthorized access. As of September 2000, the Committee was reviewing those efforts.

Noted authority Peter de Jager, who issued one of the first warnings about Y2K in Computerworld (6 September 1993), did not feel very comfortable in a 10 January 2000 interview with Computerworld about any lessons that might have been learned following the Y2K rollover event. His observations included:

- (The IT world) still does not document properly, still modifies systems instead of replacing them and still maintains a gap between itself and the business world (one of the reasons for the Y2K crisis to begin with was that IT was more concerned with technology than user needs)

- Y2K was solved, in large part, not by getting rid of the problem, but by postponing it and by using windowing instead. Windowing was a stop-gap fix, and the excuses for using it were exactly the same as those used when the two-digit year was introduced in the first place.

- Y2K will not result in better designed or better documented systems. Most organizations likely do not know or are not able to identify (1) how many different pivot dates were used in their windowing schemes, (2) where exactly they are used, and (3) documentation that defines when they absolutely must be fixed.

On 22 August 2001, the Office of the Inspector General for the Department of Defense issued an audit report entitled "Application of Y2K Lessons Learned" to assess how widely and successfully the DoD had applied the lessons learned from the Year 2000 conversion experience to other information technology programs and management issues. Since the rollover event, many DoD Components were identified as having adapted management experiences gained from the Y2K effort, and having reused and updated data compiled during those efforts such as system inventories, thin-lines, contingency plans and configuration management. The reuse and adaptation activities were largely driven by individual actions within the DoD Components and not by the DoD Chief Information Officer. As a result, according to this audit, the Components took

commendable but varied steps to use Y2K lessons learned to manage their information technology systems, while the DoD CIO missed opportunities to provide leadership in managing information assurance and information technology investments. As a result, the task of responding to congressional and OMB requirements for ensuring that systems and networks are reasonably secure, particularly with regard to the Government Information Security Reform requirements, and for complying with the Clinger-Cohen act, have been made even more difficult.

In October 2001, U.S. Senator Robert Bennett stated that "if Federal Government had not upgraded its critical systems for the Year 2000, the terrorist attacks of September 11 could have been far worse….(The) work done to eliminate Year 2000 date-change bugs and upgrade computer systems helped make rescue efforts swift" in light of the attacks. The disconcerting undertone of this "success" is that the Federal Government had dismantled its Year 2000 command center in Washington, DC after the Y2K rollover. New York City kept its in place, however, and officials were able to tap its resources when the two passenger jets hit the World Trade Center. After 200,000 phone lines failed in New York, the city and Verizon Communications restored service using procedures developed for Y2K. Bond markets reopened in two days, thanks to Y2K safeguards developed in 1999. The New York Stock Exchange used Year 2000 protocols to validate its back-up trading system. Many other organizations used Year 2000 procedures to (1) determine who to contact, (2) review the back-up of systems, (3) set up command centers and (4) direct evacuations. Bennett has proposed a Critical Infrastructure Information Security Act that is intended to:

- Secure voluntarily-shared critical infrastructure information (requiring changes to current provisions of the Freedom of Information Act – FOIA)
- Provide critical infrastructure threat analyses (requiring that information and analyses from the Federal Government be shared with the private sector in the form of notifications, warnings and strategic analyses)
- Protect those who share information (providing a narrow antitrust exemption to encourage the private sector to lead in developing solutions to common security problems)

In congressional testimony delivered 21 September 2001 before the Senate Governmental Affairs Committee, U.S. Comptroller General David Walker warned that the United States does not have a comprehensive strategy for protecting the country from cyber-attacks and terrorist threats. He indicated at that time that the Government could learn from strategies devised to deal with the Year 2000 problem. "The Y2K task force approach may offer a model for developing the public/private partnerships necessary under a comprehensive homeland security strategy." Ironically, as reported in January 2001, four of the chief DoD officials who led its successful Y2K rollover effort had retired from Government to work for information technology companies:

- **Brig. Gen. Gary Ambrose** – led the Air Force Year 2000 readiness initiative. Left in late 2000 to become IBM's DoD client director
- **Kevin McHale** – was the Marine Corps Year 2000 chief. Started working late 2000 for Mitre Corp. as assistant director for Marine Corps programs
- **Capt**. **Clifford Szafran** – led the Navy Year 2000 readiness efforts. Retired in May 2000 to serve as Electronic Data System Corp.'s program manager for the company's Naval Supply Systems Command and Naval Air Systems Command enterprise resource planning pilot
- **Ret**. **Lt. Gen. William Donahue** – was Air Force director for communication and information at AF HQ and commander of the Air Force Communications and Information Center. He became head of Computer Science Corp. business unit that deals with aerospace programs, range operations and Air Force support business.

Miriam "Mimi" Browning, who headed up the Army's Year 2000 readiness initiative was still its Principal Director, Enterprise Integration, as of January 2002.

As suggested in commentary by Bruce McConnell (former chief of information policy and technology at the Office of Management and Budget; currently a consultant) in Federal Computer Week on 7 January 2002, it still appears that many of the lessons "learned" during the Y2K effort may have fallen by the wayside:

- **Readiness Assessments**

  For the Year 2000 effort, organizations produced comprehensive inventories of their most important partners, systems and information; the functions they performed; and the interconnections between them. Firms also surveyed their suppliers to ensure their readiness.

  In post-Y2K, these inventories must be updated and maintained. Also, few organizations appear to be systematically evaluating the security posture of their trading partners. Organizations need to assess their readiness to prevent and respond to disruptions caused by cyber-attacks.

- **Risk Management Strategies**

  For the Y2K date change, organizations identified mission-critical systems and fixed them first.

  In post-Y2K, once system inventories and supplier risks have been identified, resources must be specifically allocated to address the most important risks first. Personnel security and management must also be given additional attention.

- **Useable Security Tools**

  For the Year 2000, the computer industry created tools that found and fixed the bugs.

  In post-Y2K, many technical solutions are available, but applying them to an organizations' particular solutions and systems requires a level of sophistication beyond that of most network managers.

- **Crisis Management Networks**

  For Y2K, infrastructure owners and operators organized cooperative networks to share information, exercise contingency plans and coordinate emergency response.

  Today, there is an insufficient level of information that is being shared, with the exception, perhaps, of the financial services sector, where long-standing trust relationships support strong coordination. A bill modeled on Year 2000 information-sharing legislation (not identified by McConnell, but perhaps a reference to the Bennett bill) is pending in Congress and deserves support.

- **Public Relations**

  Before the Y2K rollover, firms and industry groups organized public information campaigns to reassure shareholders and the public that the impact of the millennium transition would be minimal.

  To date (January 2002), post-September 11 corporate publicity has been limited to compassion, and has not focused on creating a coherent message of reassurance that critical infrastructures are protected and secure.

In the second annual Report Card on Computer Security (November, 2001), U.S. Rep. Stephen Horn, as chairman of the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, assigned the Federal Government an "F" (based on Office of Management and Budget reports and General Accounting Office audits) due to its failing efforts to make computers safe from cyber-attacks. As disturbing as this is, the grade is actually lower than the "D-minus" received as the overall 2000 grade. Table 28 provides an overview of the grades and the trends (higher; lower; unchanged), by agency, for the years 2000 and 2001.

Table 28: Second Annual Report Card on Computer Security (Horn)

Agency	2000 Grade	2001 Grade	Trend
Agency for International Development	C-	F	↓
Agriculture Department	F	F	→
Commerce Department	C-	F	↓
Defense Department	D+	F	↓
Education Department	C	F	↓
Energy Department	INC	F	-
Environmental Protection Agency	D	D+	↑
Federal Emergency Management Agency	INC	D	-
General Services Administration	D	D	→
Health and Human Services Department	F	F	→
Housing and Urban Development Department	C-	D	↓
Interior Department	F	F	→
Justice Department	F	F	→
Labor Department	F	F	→
National Aeronautics and Space Administration	D-	C-	↑
National Science Foundation	B-	B+	↑
Nuclear Regulatory Commission	INC	F	-
Office of Personnel Management	F	F	→
Small Business Administration	F	F	→
Social Security Administration	B	C+	↓
State Department	C	D+	↓
Transportation Department	INC	F	-
Treasury Department	D	F	↓
Veterans Affairs Department	D	F	↓
Federal Average	**D-**	**F**	↓

INC = Incomplete
Taken from Dean, J., "Feds Get 'F' in Computer Security", GovExec.com, 9 November 2001, http://www.govexec.com/dailyfed/1101/110901j1.htm (Link active as of 5 March 2002)

The National Science Foundation received the highest grade, a B+. The Social Security Administration (C+) and NASA (C-) were the only other two agencies to score above a 'D'. Sixteen of the twenty-four largest Federal agencies received an 'F', and nine of these agencies had a lower grade in 2001 than in 2000. Rep. Horn pointed out the damage caused by the Code Red and Nimda Internet worms as evidence of what can happen to computers without patched vulnerabilities and appropriate safeguards such as firewalls and antivirus software.

Subsequently, Rep. Horn and Harris Miller (President of the Information Technology Association of America) have suggested that "new senior-level management commitment is vital to ensuring that agencies have an effective department-wide computer security program to ensure that sensitive data and critical operations receive adequate attention and that appropriate security controls are in place to protect them. Attention must be given to…policy issues of cross-agency information sharing, easy citizen access to critical services and integration with state and local governments". Only then will these grades begin to improve. Necessary actions that were proposed included:

- Establishing off-site facilities for emergency backup and disaster recovery
- Developing contingency and business continuity plans
- Providing increased employee cyber-security awareness and training
- Supporting additional research on computer security and network survivability
- Developing better tools for software management
- Improving integration of information technology into physical security and access control, including surveillance and biometrics
- Greater support for education to ensure that the U.S. is developing an information security workforce in Government and the private sector with skills to keep ahead of hackers
- Improving information security at state and local governments

In November 2001 testimony before the House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Robert F. Dacey, the Director of Information Security Issues, indicated that general control weaknesses continue to be pervasive across U.S. Government Agency operations. These weaknesses are described in Table 29.

Table 29: Pervasive Control Weaknesses Across Federal Agencies (Dacey)

Weakness	Comments
Security Program Management	Each organization needs management procedures and an organizational framework for identifying and assessing risks. Poor security program management continues to be a significant problem. Many agencies had not: • developed security plans for major systems based on risk • documented security policies • implemented a testing program to evaluate the effectiveness of the controls they relied on As a result, these agencies: • were not fully aware of information security risks to their operations • had accepted an unknown level of risk by default, rather than consciously deciding what level of risk was tolerable • had a false sense of security because they were relying on ineffective controls • could not make informed judgments as to whether too much or too little of their resources was being spent on security
Access Controls	Access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss and disclosure. Commonly identified access control weaknesses include: • accounts/passwords for individuals no longer associated with an agency are not deleted or disabled, or adjusted (on a need-to-know basis) for those whose responsibilities change • users are not required to periodically change their passwords • managers do not precisely identify and document access needs for individual users or groups of users, providing overly broad access privileges to large groups of users • use of default, easily guessed and unencrypted passwords • improper implementation of software access controls, resulting in unintended access or gaps in access-control coverage As a result: • in some cases, former employees and contractors can and do read, modify, copy or delete data, even after long periods of inactivity • far more individuals than necessary have the ability to browse, and sometimes modify, delete and transfer, sensitive or critical information • insecure passwords that can be easily guessed or figured out lead to access to “high level” system administration privileges

Table 29: Pervasive Control Weaknesses Across Federal Agencies (Dacey) (continued)

Weakness	Comments
Software Development and Change Controls	Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Examples of weaknesses in this area include: • undisciplined testing procedures that do not ensure that implemented software will behave as intended • implementation procedures that do not ensure that only authorized software is used • agency policies and procedures that frequently do not address the maintenance and protection of program libraries As a result: • systems may be authorized for processing without testing access controls to ensure that they have been implemented and are operating effectively • documentation is not always maintained to demonstrate user testing and acceptance • procedures do not ensure that emergency changes are subsequently tested and formally approved for continued use, and that implementation of unauthorized software is detected and prevented
Segregation of Duties	This refers to the policies, procedures and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation to conduct unauthorized actions or gain unauthorized access to assets or records without detection. Weaknesses in this area include: • computer programmers or operators who are authorized to perform a variety of duties • staff members involved with procurement have system access privileges that allow them to individually request, approve and record the receipt of purchased items • staff members with system access privileges that allow them to edit the vendor file As a result: • computer programmers and operators have the ability to independently modify, circumvent and disable system security features • individuals independently responsible for authorizing, processing and reviewing payroll transactions could increase payments to specific individuals without detection • individuals can independently modify, circumvent and disable system security features • fictitious transactions or vendors could be used for fraudulent purposes
Operating System Software Controls	These controls limit and monitor access to the powerful programs and sensitive files associated with computer system operation. Potential weaknesses include: • inadequate controls that result in insufficiently restricted access • pervasive vulnerabilities in network configuration that expose agency systems to attack, stemming from an agency failure to (1) install and maintain effective perimeter security such as firewalls and screening routers, (2) implement current software patches, and (3) protect against commonly known cyber-attack methods As a result: • system software may be used to circumvent security controls to read, modify or delete critical or sensitive information and programs • authorized users may gain unauthorized privileges to conduct unauthorized actions, or to circumvent edits and other controls built into application programs • weaknesses diminish the reliability of information produced by all applications supported by the system and increase the risk of fraud, sabotage and inappropriate disclosure

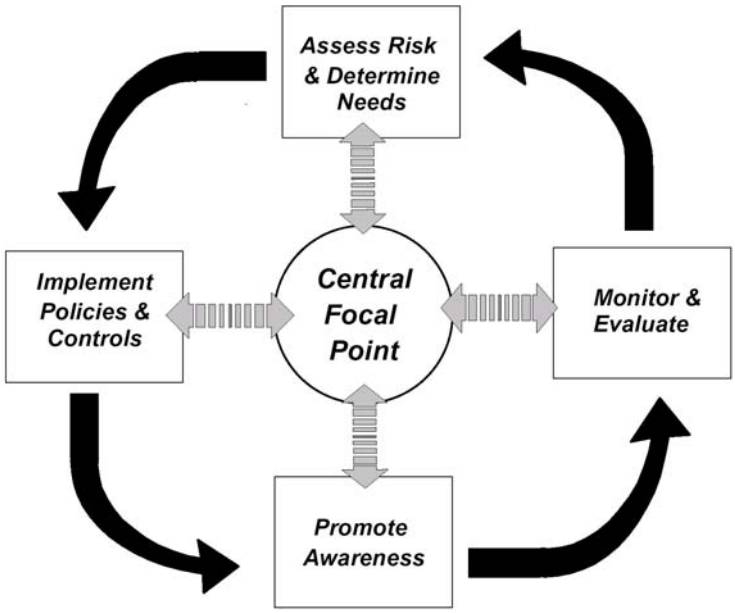
Table 29: Pervasive Control Weaknesses Across Federal Agencies (Dacey) (continued)

Weakness	Comments
Service Continuity Controls	These are controls to ensure that, when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Common agency weaknesses in this area include: • contingency plans are incomplete because operations and supporting resources have not been fully analyzed to determine which are the most critical and will need to be resumed as quickly as possible should a disruption occur • disaster recovery plans are not fully tested to identify their weaknesses As a result: • even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, inaccurate or incomplete information, or, in health care or safety system operations, potential injuries or loss of life • agencies do not perform periodic walkthroughs or unannounced tests of their disaster recovery plans, which provide a scenario more likely to be encountered in the event of an actual disaster

This same report included summarized results of a study on the practices of organizations with superior security programs, contained in report GAO/AIMD-98-68, "Information Security Management: Learning from Leading Organizations". The study found that these superior organizations managed their information security risks through an iterative cycle of risk management activities that included:

- Assessment of risks and determination of protection needs
- Selection and implementation of cost-effective policies and controls to meet those needs
- Promotion of policy and control awareness, as well as awareness of the risks that prompted their adoption among those responsible for compliance
- Implementation of a program of routine tests and examinations for evaluating the effectiveness of policies and related controls, and reporting the resulting conclusions to those who can take appropriate corrective action
- A strong, centralized focal point that can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units

Figures 11 and 12 provide an overview of this risk management cycle, and the sixteen practices identified as being employed by leading organizations to implement it.

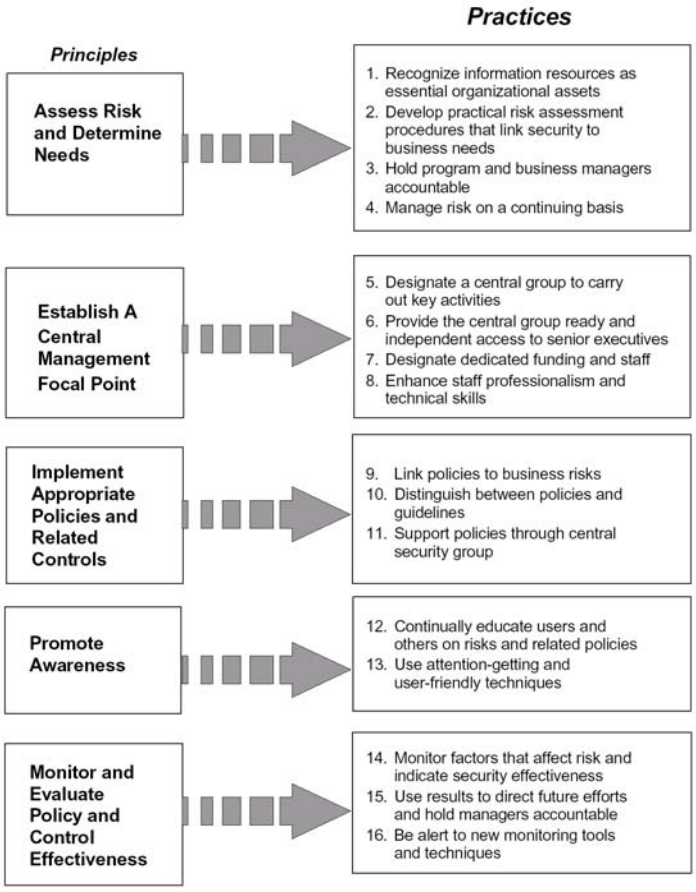


Taken from "Information Security Management: Learning From Leading Organizations", General Accounting Office, GAO/AIMD-98-68, May 1998, http://www.gao.gov/special.pubs/ai9868.pdf (Link active as of 11 March 2002)

Figure 11: The Risk Management Cycle

The GAO/AIMD-98-68 study stressed that iteration of this cycle of risk management activities was key to ensuring that information security risks were adequately considered and addressed on an on-going, agency-wide basis. Several steps that agencies could take immediately included:

- Increase awareness
- Ensure that existing controls are operating effectively
- Ensure that software patches are up-to-date
- Use automated scanning and testing tools to quickly identify problems
- Propagate the agency "best practices"
- Ensure that the most common vulnerabilities are addressed



Taken from "Information Security Management: Learning From Leading Organizations", General Accounting Office, GAO/AIMD-98-68, May 1998, http://www.gao.gov/special.pubs/ai9868.pdf (Link active as of 11 March 2002)

Figure 12: Sixteen Practices Employed by Leading Organizations to Implement the Risk Management Cycle

The Dacey testimony (GAO-02-231T) emphasized that it is imperative that information security receives appropriate attention and resources, and that known deficiencies are addressed. The steps that his testimony outlines as part of this process follow:

1. It is important that the Federal strategy delineate the roles and responsibilities of the numerous entities involved in Federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating Federal agency security, and the National Institute for Science and Technology (NIST), with assistance from the National Security Agency (NSA), is responsible for establishing related standards. In addition, interagency bodies—such as the CIO Council and the entities created under Presidential Decision Directive 63 on critical infrastructure protection—are attempting to coordinate agency initiatives. It is unclear how the activities of these many organizations interrelate, who should be held accountable for their

success or failure, and whether they will effectively and efficiently support national goals.

2. More specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Studies of best practices at leading organizations have shown that more specific guidance is important. In particular, specific mandatory standards for varying risk levels can (1) clarify expectations for information protection, including audit criteria, (2) provide a standard framework for assessing information security risk, and (3) help ensure that shared data are appropriately protected. Implementing such standards for Federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

3. Ensuring effective implementation of agency information security and critical infrastructure protection plans will require monitoring to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required in the Government information security reforms recently enacted, would allow for more meaningful performance measurement. Agencies and the Inspector Generals (IGs) have completed their first agency reviews (*as of 9 November 2001*) and independent evaluations as required by this legislation and submitted their results to OMB. In addition, agencies are also to submit plans of action and milestones for correcting their information security weaknesses. This annual evaluation, reporting, and monitoring process is an important mechanism, previously missing, for holding agencies accountable for implementing effective security and for managing the problem from a Government-wide perspective.

4. The Congress and the Executive Branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the OMB and congressional efforts to oversee the Year 2000 computer challenge.

5. Agencies must have the technical expertise that they need to select, implement, and maintain controls that protect their computer systems. Similarly, the Federal Government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical expertise is a continuing concern to agencies.

6. Agencies can allocate resources sufficient to support their computer security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on computer security will be important to ensure that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.

7. Expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As the Director of the CERT® Coordination Center testified…."It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches." In addition, in the October 31 (2001) advance executive summary of its forthcoming third report, the Gilmore Commission recommended that the President establish a comprehensive plan of research, development, test, and evaluation to enhance cyber-security.

On 13 February 2002, the Office of Management and Budget (OMB) released its first annual report to Congress on the state of Information Technology (IT) security at the twenty-four largest Federal departments and agencies. This report identifies six common weaknesses in program performance as of that date and describes the actions that both OMB and the agencies are implementing to improve IT security. These elements are summarized in Table 30. Table 31 summarizes the specific assessment of the DoD in its IT efforts.

Table 30: Six Common Weaknesses in Federal Information Technology Security

Weakness	Description	OMB Mitigation
Senior management attention	Senior leaders have not consistently established and maintained control over their cognizant operations and assets	OMB is working to promote sustained attention to security as part of the President's Management Agenda, and the integration of security into the Scorecard. Security instructions have been included in budget passback guidance, and security letters have been sent to each agency highlighting problems and specific OMB actions to assist the agency.
Measuring performance	OMB requested data to measure job and program performance, i.e., how senior leaders evaluate whether subordinates are doing their job. Virtually every agency implied that there has been inadequate accountability for job and program performance related to IT security.	OMB is working with agencies to develop workable measures of job and program performance to hold Federal employees accountable for their security responsibilities. IT security improvements will be evaluated quarterly as part of the President's Management Agenda Scorecard
Security education and awareness	Despite the law, Federal agencies continue to perform poorly in this area. Some agencies reported virtually no security training. ***DoD operates the most comprehensive security training program of any Federal agency, mandating annual IT security awareness training, providing specialized training for those with higher levels of security responsibility, and certifying all users prior to permitting access to IT networks.***	OMB and Federal agencies are working through the Critical Information Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. The CIO Council's Best Practices Committee is working with NIST through the NIST Security Practices website to identify/disseminate best practices involving security training. One of the Administration's initiatives is to establish and deliver electronic training covering a number of mandatory topics, including security, for use by all Federal agencies, as well as state and local governments.
Funding and integrating security into fiscal planning and control	Important to ensure sustained senior management attention by tying IT security to the budget process. Agency officials must ensure that security is built into and funded within each system and program through effective capital planning and investment control	OMB is aggressively applying this approach through the budget process to ensure that adequate security is incorporated directly into, and funded over, the life cycle of all systems and programs before funding is approved.
Ensuring that contractor services are adequately secure	Although laws and policy have required contractual security requirements for contractors for years, agency reports reveal ongoing weaknesses (e.g., no security controls in contracts, or no verification that contractors fulfill their contractual requirements) ***The DoD has been recognized for the significant work that it has done in ensuring that contractor-provided services are adequately secure and meet current security requirements.***	Under the guidance of the OMB-led security committee established by Executive Order, an issue group is to develop recommendations that include how security is handled within contracts. OMB is to work with the CIO Council and the Procurement Executives Council to establish a program that ensures appropriate contractor training in security.

Table 30: Six Common Weaknesses in Federal Information Technology Security (continued)

Weakness	Description	OMB Mitigation
Detecting, reporting and sharing information on vulnerabilities	Too many agencies have no meaningful system to test or monitor system activity and, as a result, are not able to detect intrusions, suspected intrusions, or virus infections.	GSA's Federal Computer Incident Response Center reports to OMB on a quarterly basis regarding the Federal Government's status on IT security incidents. Under OMB and Critical Infrastructure Protection Board guidance, GSA is exploring methods to disseminate security patches to all agencies more effectively.

Table 31: FY 2001 Performance – DoD Information Security Reform

Topic Area	Description
Security funding	• Planned FY02 funding for IT security and critical infrastructure protection is $1.77B, over twice all other agencies/departments budgets combined • Funding level is 7.5% of total planned IT portfolio • DoD total IT portfolio is roughly equal to all other agencies/departments combined
Number of programs reviewed	• DoD maintains an "IT Registry Database of Systems" that lists over 3,700 systems, each of which has a designated function and manager • A statistical sample of 560 classified and unclassified systems was selected for review • The DoD IG, in collaboration with the Army and Air Force audit agencies, reviewed 90 major applications from a total population of 4,939
Review and independent evaluation methodology	• DoD has formally established an IPT to develop IT security review guidance for DoD bureaus, branches and agencies (i.e., Components) • The Components provide assessment data which the IPT aggregates into an "assessment of assessments" to meet Security Act reporting requirements • DoD used a combination of methodologies to develop a matrix of standard reporting elements based on (1) the NIST self-assessment guide, (2) the DoD IT Computer Security and Accreditation Process and (3) other DoD assessment vehicles • These methods were applied to the 560 systems sampled from the IT Registry • The DoD IG's primary evaluation method was to identify which applications in their sample were certified and had designated security personnel, augmented by a review of prior DoD, IG and GAO reports for information related to OMB reporting guidance questions
Material weaknesses	• DoD identified cumbersome IT management processes and outdated IT policies as material weaknesses in its IT security program • As a result, DoD is having problems implementing policies that are relevant to a rapidly changing IT environment • Relying on general reviews during the budget cycle is no longer adequate to ensure IT security for new systems whose number of vulnerabilities and security threats have increased dramatically

Table 31: FY 2001 Performance – DoD Information Security Reform (continued)

Topic Area	Description
Measures of performance used to ensure that officials assessed risk, determined security levels, maintained plans and tested controls	• The DoD report does not identify the measures of performance used to ensure that officials have assessed risk, determined security levels, maintained plans and tested controls • The report does not provide any examples of how the DoD has performed in these categories • The report identifies 4 phases of mandatory activities used for the certification process (definition, verification, validation and monitoring), but the IG found that these security policies had not been fully implemented (60% of the reviewed applications lacked certifications) • Failure to implement these policies due to unclear definition of security parameters and responsibilities, compounded by limited DoD-level and Component head oversight, and the practice of approving different organizations to develop, operate and use IT applications • IG noted that although the Army had developed some performance measures, they only applied to one of the information security categories (testing) and, in 79% of the evaluated Air Force applications, no performance was measured in any of the categories
Measures of performance used to ensure that the CIO has effectively implemented and maintained security programs and trained employees	• Report describes several specific areas where the DoD is performing IT security practices, but gives no examples of performance measures, or actual performance in these areas • Absence of specific DoD performance measures hampers the Secretary's ability to oversee and ensure that the CIO is adequately maintaining a DoD-wide IT security program • Mechanisms have not been established to provide oversight or comprehensively measure compliance to DoD Directive 5200.28 • Although an IPT was established to evaluate and consolidate data to report the DoD IT security posture, they did not develop a plan to consistently apply information security requirements across all DoD systems and networks
How the agency ensures employees are sufficiently trained	• DoD policies mandate annual IT security awareness training for 3.4 million military and civilian employees, specialized training for employees with significant IT security responsibilities, and certification of all users before allowing access to IT networks • Established a Human Resources Development Functional Area to implement personnel awareness training for information security • Employee awareness training is tracked, with up to 96% of personnel having received awareness training • DoD does not distinguish IT security training from other types of training, so costs could not be tracked, nor did they report how many personnel were determined to require awareness or special security training, or actually received specialized training (and the related costs)
Department documented procedures for reporting and sharing vulnerabilities	• DoD has a fully functional and effective incident response capability • A succinct summary of the criteria for reportable incidents, and the reporting process used within the DoD and externally with national incident response coordinators, are provided within the report • The report also contains meaningful performance measures and actual results (e.g., 29,281 reportable incidents of which 384 resulted in unauthorized access) • 384 unauthorized accesses resulted in 194 investigations leading to 24 criminal indictments, resulting in 18 convictions • DoD incident detection, handling and vulnerability-sharing capability are the best among all Federal departments and agencies

Table 31: FY 2001 Performance – DoD Information Security Reform (continued)

Topic Area	Description
Department integration of security and capital planning	• DoD stated it was unable to provide information on whether IT security requirements and costs were identified on capital asset plans submitted to OMB, but the report does describe the investment control strategy that is used to integrate IT security with capital planning • DoD currently devotes 60-75% of their information assurance resources to their Information Systems Security Program, which is subject to annual review
Critical asset prioritization and protection methodologies	• DoD has no department-wide methodology to identify and prioritize critical assets, or their dependencies on key external systems, in order to protect them within its enterprise architecture • Existing methodologies/capabilities vary widely across DoD Components, and are tailored to meet their specific needs • DoD did not discuss implementation of a department-wide methodology, or the adoption of an existing methodology such as Project Matrix (which compiles data from all agencies to support gap analysis across the Government's enterprise) • IG observed that DoD has in place an information technology registry of over 3700 critical assets, but found that not all assets are registered. It as also noted that the IG did not review the overall effectiveness or completeness of the IT registry.
Measures of performance used to ensure the security plan is practiced throughout the life cycle of each system	• The report claims that standardized information assurance metrics are defined in Joint Chiefs Instruction 6510.04, but this Instruction is in review and no specific examples of metrics are given • Only examples of performance measures are system security evaluations, operational assessments of system usefulness, and the number of certified system administrators • No actual performance data is given • DoD has several vehicles in place to assess information assurance, but no way to evaluate and consolidate information assurance data to report its information security posture, without which it cannot measure performance of information security throughout a system's life cycle
Integration of information technology, critical infrastructure protection, physical, and operational security programs	• DoD indicates that the Critical Infrastructure Protection Plan (CIPP) documents the processes that ultimately ensure the reliability of physical and information infrastructures • The report does not provide specifics on how the DoD Components integrate the various security elements of their assets other then to state that risk assessments are conducted after assets are identified • This is intended to provide asset owners with a catalyst for vulnerability mitigation, minimizing operational impacts, and development of risk management protocols
Department methods to ensure that contractor services are secure	• DoD employs a variety of methods to safeguard the security of contractor-provided IT services, including specific language on contractor security procedures in every contract • DoD also relies on investigations, audits, and background screening and training for contract personnel • The IG cited several examples of security breaches in contractor-provided services, most notably in the area of contractors, including foreign nationals, who were granted access to systems without appropriate background investigations • The IG findings show that there is need for improvement in this area, but that ***overall the DoD is stronger in this area than most other Federal departments and agencies***

8 Summary and Conclusions

This Critical Review/Technology Assessment has described work that was performed by the Data and Analysis Center for Software (DACS) (Contract SPO700-98-D-4000) in support of the Office of the Deputy Under Secretary of Defense for Science and Technology (ODUSD(S&T)) over the calendar time period 12 May 1999 through 31 May 2002. The report represents the culmination of efforts performed under DACS Technical Area Task (TAT) 19, CLIN 0002 Delivery Order 0018 (DA-99-0010/0024) entitled "ODUSD(ST) Y2K Analysis and Support". The scope of the effort evolved over the period of performance. Its original intent was to provide support and analysis to the Special Assistant for Computing and Software Technologies, Office of the Deputy Under Secretary of Defense (Science and Technology) (SACST/ODUSD(S&T)) in assessing the Year 2000 (Y2K) readiness of selected systems within the Service Laboratories, High Performance Computing Centers (HPCCs) and Department of Defense (DoD) Modeling and Simulation (M&S) programs, and to provide the necessary support needed in reporting and analyzing Y2K End-to-End (E2E) testing plans, procedures, reports and results. Due to the success of the Y2K rollover, the scope of the project was first extended to include Y2K lessons learned and, subsequently refined to assess how Y2K lessons learned could benefit Critical Infrastructure Protection initiatives.

After years of preparation, millions of person-hours expended, and billions of dollars invested, the lack of any "significant" Y2K problems left the door open for critics to claim that the Year 2000 crisis was substantially overblown and exceedingly wasteful. Those organizations and people most closely associated with this massive undertaking, however, have a much greater understanding and appreciation of how critical the success of this effort was to our national interests, as well as to the global community as a whole. Even a cursory review of some of the events that did happen – prison cells unlocking, disruption of financial services and transactions, the need for manual intervention at nuclear power facilities – should cause skeptics to realize how catastrophic the Y2K rollover might have been for a world totally unprepared to handle it.

As a minimum, the Y2K effort served as a model for how complex technological problems having high levels of interdependency and risk should be handled. As described in this report, there have been numerous lessons that have come out of the Y2K effort, from both government and industry, that need to be leveraged in order to adequately support critical infrastructure protection initiatives. At the highest levels, these include:

- the need to assess and address IT issues as business and management problems, rather than strictly as technology problems, in order to find technologically sound, yet cost- and time-efficient, solutions

- the need to fully research, understand and communicate the existing and potential future vulnerabilities of IT in order to adequately prepare risk assessment and management plans to eliminate or mitigate those vulnerabilities

- the need to fully research, understand and communicate the existing and potential future interdependencies of IT in order to be able to "fix" your own organization, as well as all "global" organizations upon which you depend for support and service

- the need for commitment from senior levels of management in both the public and private sectors to proactively provide the leadership, experience, guidance, resources and tools necessary to address and solve pervasive and persistent IT problems

- the need to establish a centralized resource that leverages public/private partnerships to coordinate and communicate issues, data, information and solutions on a national scale in order to get the right information to the right people at the right time

- the need to maintain up-to-date inventories of system assets and a full understanding of which assets are "mission-critical", "mission-essential" and "non-mission essential" so that risk mitigation, contingency, and continuation of service efforts can be prioritized and focused on the "critical few", as opposed to the "trivial many"

- the need to develop and actively maintain all documentation, particularly risk assessment/management plans, contingency plans, and continuity of operations plans, that will assist in the identification of (and recovery from) potential critical infrastructure IT catastrophes

The most critical concern coming out of the Y2K experience is, however, how much has really been learned at all in the context of preparing the nation to defend itself against what are undoubtedly inevitable cyber-attacks in the future (remembering that the future is "now"). It has been several years since the country embarked on its Critical Infrastructure Protection mission and, from a post-9/11 perspective and review of the current available literature, progress has not been as fast or as effective as it must be to counter the attacks experienced over the last several years, and the perceived uncertain threats of the coming weeks/months/years. The lessons learned from Y2K, as described above and in more detail within this CR/TA, have not been applied to critical infrastructure protection with the same sense of urgency and coordination as they were when developed and implemented under Y2K. In the pre-9/11 environment, this relative complacency and slow progress may have been politically understandable. In the present environment, this complacency should no longer be tolerated. In this context, the Computer Security letter grade of "F" assigned to the Federal Government by the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations in November 2001 must serve as a wake-up call to take the issue of our national cyber critical infrastructure protection more seriously.

Appendix A – The International Y2K Glitch Report

Country	Y2K Glitch
Australia	A woman at a very small real estate brokerage in the Sydney, Australia area said they are having more and more Y2K problems everyday
Australia	Ambulance officers have met with union officials after claims mobile computer units in their vehicles began to routinely fail.
Australia	Computer problems are delaying the opening of the Domain Tunnel.
Australia	Electronic Parking Meter at North Sydney Oval is displaying the Year as 1900 on the LCD display
Australia	Parking Meters in Sydney showing date as 01/03/1900
Australia	Power and phones went out in Queensland
Australia	Public Transport ticketing system failed in Tasmania and South Australia
Australia	Qantas jet carrying 68 passengers was forced to make an emergency landing at Darwin Airport.
Australia	Sydney Bank Computers
Australia	Telstra Corp. reported phone failures in South Australia, primarily New South Wales and Victoria. Also, Microsoft Excel spreadsheets are experiencing software glitches.
Australia	There has been widespread anecdotal evidence of localized Y2K glitches in Australia alone, from invoices not being sent out on time, to erroneous date calculations and computer system glitches.
Australia	Thousands of litres of sewage have spewed into the Maribyrnong River downstream of Cordite Avenue in Melbourne's west.
Bermuda	The Bermuda Stock Exchange reporting system malfunctioned
Bolivia	Customs failure at Puetro Suarez, Land property registration glitches, minor glitches at a public office in Cobija, health diagnosis equipment failure, and accounting software (SINCOM) failed. All fixed.
Brazil	Brazil's key Santos port experienced a computer hiccup in its customs process
Brazil	Hospital appointment scheduling system failed
Brazil	Part of a 12-mile pipeline from the Duque de Caxias refinery sprung a leak near the coast
Brazil	Problems with printers in convenience stores in Sao Paulo.
Brazil	Reports of glitches in toll roads
Brazil	The Viracopos airport in the interior of Sao Paulo state experienced a computer problem in its customs process
Bulgaria	Passport agency computers in Bulgaria issued passports with incorrect dates.
Canada	A computer problem forced the newly created Canadian Venture Exchange for small equity firms, known as CDNX, to suspend trading for nearly three hours on Friday
Canada	A malfunctioning computer system has led to thousands of Toronto public school employees working without pay or only partial pay since the beginning of the year.
Canada	A Y2K glitch caused yet another Bell Canada system to crash, leaving thousands of Ontario businesses and residences without phone service.
Canada	Cell doors failed in Mountain Penitentiary in Bristish Columbia
Canada	Computer glitch hits Saskatoon billings
Canada	Halifax jail lets robber free one year early
Canada	Nova Scotia drivers with old drunk driving convictions were sent reminders to mend their ways
Canada	Rogers Cable slammed Ontario wrestling fans last night when its pay-per-view network went down the tubes.
Canada	Security access system at Canada's National Defense Department offices in downtown Ottawa failed
Canada	Small computer glitch on Friday at the website of Network Solutions Inc., the U.S. company registering dot-com website addresses.
Canada	The Leap Year bug leaped into action on Tuesday, shutting down the City of Montreal's taxation computer system
Canada	Three workers at an auto testing plant near Montreal were killed today
Canada	Toronto 911 system was out of service for 5 hours
Canada	Toronto Stock Exchange customers using Netscape browser software to call up personal portfolios
Canada	Toronto Transit telephone hotline is closed
Canada	Wage fiasco leaves school staff unpaid
Chile	Blackout hits north Chile, cuts power to mines
China	ATM system failed
China	Bank computer error
China	Branches of the People's Bank of China had their internal and enterbank e-mail systems fail
China	Department store computer systems
China	Guangming Daily's website date program error
China	Hainan pharmaceutical factory suffered a crash caused by 9/9/99
China	Health Care systems
China	National Meteorological Administration observation systems in Ningxia failed
China	Taxi meters in Jiangsu Province blanked out
China	The Beijing Morning Post reported that renowned writer Gu Qingsheng lost all his computer data due to the Y2K bug.

Country	Y2K Glitch
China	The Beijing Youth Daily, reported that some automatic teller machines in the southern city of Guangzhou failed to dispense cash and that some bank computers are still dating documents with the year 1900 instead of 2000.
China	The central bank says there were some disruptions in remote Qinghai province, involving the internal interbank electronic mail system
China	The website www.2000.com.cn can not be accessed during the transition time, and the web
Congo	Y2K bug hits Congo's finance ministry's salary system
Costa Rica	Costa Rica was successful in overcoming the feared Millennium Bug, Science and Technology Minister Esteban Brenes asserted.
Costa Rica	Ministry of Science and Technology reported minor problem in billing system at a petroleum refinery.
Denmark	Tele Denmark has problems with E-mail
Denmark	Unidanmark A/S bank's Unitel payment and information system failure
Egypt	British Petroleum Company has a BIG Y2K problem. It happened just after the rollover where they were monitoring it in their crisis center.
Egypt	Three dialysis machines stopped functioning
Europe	AVL Omni 9 blood gas analyzer failed
Europe	Datascope Passport ELXG patient monitor malfunctioned
Europe	E-commerce date validation routines mismatches
Europe	Elekta Sli linear accelerator malfunctioned
Europe	Kendall Aerodyne Ultratherm humidifier failed
Europe	Marquette ST Guard computer (ECG trend monitor)
Europe	Organon Teknika Ltd. Bactalert blood culture incubator detector malfunctioned
Europe	Oxford Sonicaid FM6 fetal monitor malfunctioned
Europe	Siemens Sirecust 455-1 data management system failed
Europe	Sorin Biomedical (Cobe) perfusion controller malfunctioned
Europe	Stericare Sterilog autoclave printer malfunctioned
Fiji	In Fiji the Immigration Ministry has unexpectedly and without explanation turned off its computers. Other ministries were asked to do likewise.
France	A spokesman of Cigref pointed out that the passage to year 2000 had proceeded particularly well: "on average, we recorded 10 anomalies per company member
France	Syracuse II military satellite glitch found at ground stations relating to communications
France	The bug of February 29 however threatened a moment many the Parisian parking meters, which had to be reprogrammed one by one.
Gabon	Isolated glitches popped up in some accounting systems.
Germany	Berlin fire department's computer system problems
Germany	Berlin Opera payroll system malfunctioned
Germany	Bruehl Train Disaster Damage Exceeds 50 Million Marks
Germany	Cologne Bank computers reporting balance errors.
Germany	Deutsche Bank international clearing system failed
Germany	German banks software malfunctioned
Germany	Only Minor "Y2K" Casualties in Germany
Ghana	Several private individuals have approached the National Y2K Secretariat for assistance in fixing malfunctioning equipment
Ghana	Some equipment at the Cardiotherapy unit of the Korle-Bu Teaching Hospital malfunctioned
Greece	Older model cash registers malfunctioned
Greece	Passport agency computers in Greece issued passports with incorrect dates.
Greece	The tax information system TAXIS has been down. All computerized regional state finance offices have been affected.
Grenada	A compliant version of the computer systems for customs services was not commissioned as of Dec. 30, 1999.
Grenada	Only the payroll (internal) component of the sole provider of water in Grenada, the National Water and Sewage Authority (NAWASA) was not compliant.
Guam	Guam federal food stamp benefits systems malfunctioned.
Guatemala	At least 35 small and medium sized businesses have suffered Y2K problems
Honduras	Regional customs house computer systems failed
Hong Kong	A blood sample analysis machine displayed wrong dates, but the machine still functioned.
Hong Kong	A LAN used by a training department had a file created after the millennium rollover that showed a creation date year 2028 instead of 2000. Other functions remained normal.
Hong Kong	Bank computer's error Tuesday made instant billionaires of some customers - but only for a few hours.
Hong Kong	Glitches were reported in "breath-testing" equipment for sobriety checks.
Hong Kong	The computer system controlling the options pricing system of the open outcry system for the trading of Hang Seng Index options contracts encountered date-related problems shortly after the opening of the market on January 4.

Country	Y2K Glitch
Hong Kong	Three government agencies reported Y2K problems, Agriculture and Fisheries, Civil Service T&D Institute and Auxiliary Medical Service
Hungary	Around 500 calls for help were made to the Millennium Command Center on January 3, 2000 from small enterprises
Hungary	ATM machines could not be used at one of the biggest retail banks
Hungary	One process control system in a manufacturing company failed on start-up
India	Bombay Stock Exchange's trading system malfunctioned
India	New Delhi lost power
India	New Delhi lost power
India	Northern grid for New Delhi collapsed again
India	Small trader record system failed
India	Stock broker systems failed
Indonesia	Central Bank Clock displayed the year 1900 shortly after midnight, but was quickly fixed.
Iran	A passenger airliner and a military transport plane collided at Tehran Airport
Iran	In one of the hospitals in Tabriz province, a blood gas analyzer which was not switched off before rollover changed to 1900 and did not function properly.
Iraq	Iraq oil exports fell by two thirds from last week's export totals
Ireland	Eircom automated dial-in service malfunctioned
Israel	Defense, public and government institutions and banks reported minor Year 2000 problems.
Italy	Bari Central Court GIPS office has had all 1999 records erased and staff time clocks have ceased to function
Italy	Foggia local health authority staff records system failed
Italy	Judicial Departments in Naples, Venice, Genoa and Rome had computer system problems
Italy	Lazio Region Health registry had malfunctions
Italy	Monterosso Calabro and Pimentel Registrar's offices computer systems malfunctioned
Italy	Rome Sewage System
Italy	Sicilian court system computers added 100 years to jail terms
Italy	Trento Road Vehicle Registry failed
Jamaica	Capital City traffic light system non-operational
Jamaica	Computerized traffic lights out in Jamaica
Jamaica	Year 2000 snafus occurred in computerized traffic lights at eight intersections.
Japan	12 Japanese brokerages have had minor problems with software developed by Nomura
Japan	8 Japanese banks and 2 small financial institutions experienced minor computer problems
Japan	An aviation computer system, which collates flight and weather information for small planes and helicopters, experienced minor problems.
Japan	Another glitch materialized when ATMs stopped working
Japan	Automated teller machines at post offices shut down.
Japan	Computers at six observatories in Tokyo and other cities failed to correctly recognize Feb. 29.
Japan	Data storage program failed at the Onagawa Nuclear Power Plant
Japan	Horiba, Inc, found that the Sera-520 model electrolysis analyzer malfunctions
Japan	Japanese weather stations reported heavy rainfall when none actually fell
Japan	Malfunctions reported at nuclear power plants
Japan	Monitoring system for 185 control rod location alarm - Fukushima No 1 reactor
Japan	Post office registered mail tracking system failed
Japan	System sending data on plant status to ITIM malfunctioned
Japan	Tokyo Electric Power Co. data storage program failed
Japan	Tokyo Electric Power reported monitoring failure, with a total of 22 reports of minor failures in power system computers
Japan	Tokyo's Katsushika Ward chemical plant leaked sodium hydroxide solution
Kazakhstan	Ekibastuz Hydroelectric Power Station-2 has handled its technology processes manually since Jan, 1, 2000,
Kazakhstan	In one of the government buildings, a Y2K problem occurred in the system that controls air conditioning, elevators, etc.
Latvia	Latvia customs office system reverts to 1900
Malaysia	Reports of problems with billing system in the software programs in several Land offices, and also problems related to wrong dates in the petrol/gas pump display panels of several petrol stations in the country.
Malaysia	Reports of Year 2000 glitches in defibrillators and heart monitors were noted.
Malaysia	Satellite TV transmission was cut at midnight in the Penang area
Mali	The ferry system experienced a Y2K breakdown for its Dakar/Bamako itinerary. The information system, developed by CNUCED is used to monitor transport of merchandise. In addition, the ticket dispensing system had also broken down due to Y2K.
Mali	The monitoring of Mali's railway system has been disrupted by computer problems
Mexico	Some medical equipment (ultrasound, X-rays, clinic analysis) did not date function correctly.
Moldova	Some minor problems occurred with computers resetting dates to 1994. Problem was fixed easily.

Country	Y2K Glitch
Mongolia	A few railroad ticket counters with outdated computer systems could not function on Jan. 3.
Namibia	Ministry of Home Affairs population register system failed
Namibia	Radio station ‘experiences problem with advertising scheduling computer
Namibia	Some civil servants went without pay for February, others received only a portion of their salaries while all are without pay slips due to a computer glitch in Government's pay system.
Nepal	Personal appliances affected by rollover
Netherlands	a computer in the Netherlands could not transmit weather to the media
Netherlands	Dutch Bank ABNAmro's OfficeNet (online banking) has a Y2k problem with exports of payment data.
New Zealand	a localized problem with electronic banking systems. 4000 eftpos terminals hit by Leap Year hiccup
New Zealand	Blackout for 200,000 households in South East Queensland
New Zealand	Passengers and planes were stranded at airports across the country on December 22 when crucial communication links between air traffic controllers crashed.
New Zealand	The admitted Y2K problem is in the DOS version of an accounting package named Pacioli.
New Zealand	THE country's air traffic control system broke down again last week -- the second time in a month -- but the Airways Corporation is playing down safety concerns.
New Zealand	Wellington Bus-Pass validating machines malfunction
Nicaragua	Supreme Court and Ministry of Agriculture reported Year 2000 failures at approximately 800 midsize companies.
Nigeria	A minor Year 2000 glitch occurred in the Port Harcourt refinery maintenance and material management system. T
Nigeria	Reported to have experienced difficulties in the energy sector.
Nigeria	Some noncompliant private telephone operators were disconnected due to Y2K problems on 31 December 1999
North America	Financial Crimes Enforcement Network (FINCEN) is not Y2K compliant
North America	GE/Marquette Midas 2100 cardiac catheterization physiologic monitoring system failed
North America	Hach BodTrack monitor malfunctioned
North America	Life-Tech Urodynamic computer system (urodynamic measurement system) malfunctioned
North America	Lotus Notes Y2K problem
North America	Marquette MGAPC medical gas analyzer malfunctioned
North America	St Jude Medical PR-3500 pacemaker programmer malfunctioned
Norway	105-year-old offered space in Norway kindergarten
Norway	National Heritage Director fears that public archives in Norway have been lost
Norway	Train signals malfunctioned in Norway
Pakistan	Customs clearance of imports was delayed for two days due to a fault in the computer system of the Customers Service Centre at the Karachi Customs House
Pakistan	Islamabad Stock Exchange systems failed
Philippines	Cases of fax machines or other non-critical electronic equipment displaying the wrong date were reported.
Portugal	Hospital admissions and payment systems experienced minor date-change problems.
Portugal	Several problems were discovered.
Romania	In what may be Europe's worst environmental disaster since Chernobyl, a cyanide spill contaminating a major river has moved into Yugoslavia and destroyed all life in the water
Russia	A train on the St. Petersburg-Moscow railway link crashed into the back of a freight train on Wednesday morning, killing one of the drivers and injuring 15 passengers who were traveling from Veliky Luki to St. Petersburg.
Russia	Kremlin Press Office e-mail system failed
Russia	Minor glitches in management systems in Russia nuclear power plants reported.
Russia	Vladivostok, 28th January: Serious fuel shortages in Maritime Territory in the Russian Far East have resulted in a critical situation in power supply to the Territory.
Rwanda	Government reported failure in customs system because of Year 2000.
Saudi Arabia	Medical equipment (e.g., electrocardiogram, ultrasound and Arterial blood gases machines) showed date function problems. Some locally-designed software experienced glitches with Muslim to western date functions.
Scotland	Gambro haemodialysis machines (models AK100&AK200) affected
SE Asia	Cartiotocograph from Oxford Instruments malfunctioned
SE Asia	Delta Computer patient administration system failed
SE Asia	Nihon Kohden defibrillator malfunctioned
SE Asia	Satchwell Building automation system failed
Singapore	Singapore: Shell Cuts Pulau Bukom Refinery Production
Singapore	the Singapore subway system rejected some riders' cards.
Slovakia	On the web page exchange of one bank, an incorrect date was displayed on January 3rd. The same thing happened to a weekly magazine on January 5th.
Slovakia	The unikart payment system, the LBS Company, crashed
South Korea	Aluminum manufacturing plant affected by Y2K

Country	Y2K Glitch
South Korea	Ansan Severance Hospital and Dongshin Hospital in Kyonggi Province yesterday reported that a computer-controlled marrow measurer malfunctioned
South Korea	Apartment Building reported heat and hot water loss due to Y2K.
South Korea	Factory in Ch'angwon industrial complex had to stop operation for about 4 hours on 3 January 2000
South Korea	One type of medical device (density measurement) failed.
South Korea	The patient registration program at Ansan Severance Hospital malfunctioned
South Korea	There were 16 confirmed cases of Y2K glitches in the country as of the afternoon, of 3 January according to the ministry of Information and Communication .
South Korea	Tongsan Medical Clinic in Ansan and Pak Sang-Hyon Medical Clinic administration system malfunctioned
South Korea	Total of 12 Y2K-related problems were reported in small shops, video-rental shops, pharmacies and hotels.
Spain	Foratrom reports that there was one nuclear power plant with a minor computer problem
Spain	Reported to have experienced difficulties in the energy sector.
Sri Lanka	Monitoring unit of an electrocardiogram machine at a hospital.
Sudan	The interbank communications in two banks (out of 10 major banks) was delayed by two days due to Y2K problems in the communications software (an old Novell version).
Sweden	Swedish hospital reported its computers lost access to patient information.
Sweden	The comprehensive reporting system indicated , up to mid-January 2000, 87 minor Y2K-related glitches reported in health care (unable to register newborn, parking meter problems, isolated cash registry failure, computerized entry to a sport center not working, and control and surveillance system problems in a water treatment plant.
Taiwan	A blood pressure monitoring machine displayed wrong dates in one hospital in southern Taiwan.
Taiwan	Bad date codes in hospital registration systems reported.
Tajikistan	A few executing (.exe) files needed to be updated to become Y2K compliant.
Tanzania	Zanzibar reported television transmission problems.
Thailand	Meteorological Department experienced a minor glitch
Thailand	Stock Exchange of Thailand computer glitch
Thailand	Thailand Millennium Center had received about 341 inquires on problems
Turkey	Oil pipeline systems malfunction
Turkey	Some minor Y2K glitches in the health care sector, including blood sample analyzing machine, patient monitoring equipment, ultrasonic device, tomography device and dialyses machine, were reported
Uganda	Nakawa Inland Port computer system failure
Uganda	Y2K problem at Uganda inland port.
UK	A fault on British Telecom's network prevented customers from dialing in to hundreds of free Internet service providers, potentially affecting millions of Internet users.
UK	Aberdeen weather centre found the bug had affected its observation equipment.
UK	Bactalert Blood Culture incubator
UK	Befordshire County system for tracking age of residents malfunctioned
UK	Benefits glitch hits Coventry City Council to seek compensation from Sanderson
UK	Cybex Isokinetic Machines (used for measuring muscle performance)
UK	Firm has several computers (Award BIOS 4.51PG) showing a date of 2/1/80 when rebooted since January 20, 2000
UK	Foratom reports that there were two nuclear power plants with minor computer problems
UK	Halifax Police system malfunctioned
UK	Ikea store cards fail Year 2000 test
UK	Independent Energy faces billing snag
UK	Inland Revenue had some 4,000 notices sent out dated 4 January 1900
UK	Inland Revenue's electronic lodgment system (ELS) has encountered Y2K incompatibilities with users of Digita's tax software.
UK	Linear accelerator (Elekta Oncology Systems, Ltd.)
UK	London Dockland Light Railway system
UK	Milk pasteurization plant found that its system would not record processing heat and timing information for dates after December 31, 1999
UK	National Statistics Office computers were printing 22002000 on birth certificates. LONDON (Reuters) -
UK	Office for National Statistics poll of 1114 UK companies shows Y2K problems
UK	Oldham Chronical newspaper system malfunction
UK	QA Software for X-ray films
UK	Racal Electronics Plc credit card swipe machines malfunctioned
UK	Royal Doulton China and Glass maker warehouse management software system failed
UK	Royal Opera House has suffered a further setback with the cancellation of another performance, the ninth since it reopened in December
UK	Sage released a statement explaining why users of its 1997 Sage Instant Accounts package had experienced date change problems.
UK	Some bugs remain in electronic tax filing software in U.K
UK	Sonicaid foetal monitor

Country	Y2K Glitch
UK	Telephone system failure
UK	The 28 reported technical defects suffered by "minor systems" in nuclear plants occurred Japan, Spain, Great Britain and the United States
UK	Treatment planning software failure
Ukraine	A reactor at Ukraine's Yuzhnaya atomic power plant was shut down after a malfunction Wednesday, nuclear officials said. It was the fourth unplanned reactor stoppage this week.
Ukraine	Programs of the Ukrainian national television channels UT-1, UT-2, and Inter, have not been broadcast to 3/4 of the territory of Sumy oblast since noon January 11.
US	25% of 1750 IT professionals noted that their organizations had suffered Y2K problems
US	A Coast Guard system that archives electronic messages had trouble.
US	Amtrak system that monitors train progress, arrivals and departures failed
US	An alarm failed to alert workers that a pump supplying water to indoor incubators had shut off during the night
US	Animal Control/License system malfunctioned
US	Apple Computer Inc. said on Tuesday that the Y2K bug caused a few minor malfunctions in its information technology systems
US	At HUD, minor problems surfaced during Electronic Data Interchange (EDI) retrieval of files
US	ATT billing system malfunction?
US	Audio Box Amps Pro interface software custom algorithm failed
US	Bank credit card companies reported they have identified potential Y2K glitch involving some credit card transactions. Merchants did not make use of free upgrades for a CyberCash, Inc. software package. The glitch could result in duplicate postings after January 1st.
US	BellSouth reported some minor internal glitches
US	Bureau of Alcohol, Tobacco and Firearms had computer system problems
US	CADEC truck computers malfunction
US	Cash register in Okinawa Federal store had Y2K-related problems
US	Cash registers crash at Petsmart
US	Chevy Chase Bank (Washington, DC) customers hit snags
US	Chloe's Tents and Events store computer system failed
US	CSX Trains frequently arrive late. Cargo cars supposed to be full are coming in empty. Customers are asking for refunds and demanding answers
US	Delphi.com server has problems
US	Department of Energy facilities Y2K problems
US	Dial Data provider system
US	DOD Intelligence System failed
US	Due to Y2K issues, ftyyourmoney.com had to shut down the FTQUICKEN Portfolio tool
US	E*Trade customers had sporadic access to their accounts, preventing some customers from making online trades for about 30 minutes
US	East Coast airports FAA host computer systems crashed
US	E-mail problems continue for Avista customers
US	EPA ERNS database turned off on December 31 due to Y2K problems
US	Equipment failure at [MindSpring Enterprises] left more than 1 million computer users unable to send or receive e-mail for about two hours Thursday
US	Federal Emergency Management Administration (FEMA) experienced a Y2K problem with a database of reservists and regular staff
US	Federal Housing and Urban Development Administration reported minor glitches with some of their systems
US	Firestone Tire and Service Center computer system failed
US	First Union Bank sent notices dated 0001
US	For the past week to ten days experiencing problems with phone calls
US	Foratom reports that there were seven nuclear power plants with minor computer problems
US	Four systems at the Federal Housing Administration experienced minor Y2K-related problems late in the day on Jan. 3.
US	Gas station at-the-pump system error
US	George and Bill's Appliance Service UCC Statement
US	Hershey Foods supply system disrupted
US	Housing and Urban Development department reported the Tenant Rental Assistance Certification system malfunctioned
US	Insurance company automatic debit program error
US	Interland.net had failures of at least three servers
US	IRS notes that lots of people have not gotten their tax forms through the mail
US	Lake County, , Dial-A-Ride computer failed
US	Local auto service shop smog check system
US	Local Video store computer crashed

Country	Y2K Glitch
US	Lots of new Cisco Field Notices including Y2K labeled
US	Major musician's magazine and warehouse ordering system malfunctioned
US	MSC/Premera Blue Cross: In September of 1999, we transitioned to a new claims processing system to comply with Y2K standards as well as serve you, our customers, more efficiently.
US	MSNBC visited accounting.CIHost.com Thursday and was able to generate about 1,500 customer records dated from March of last year through Wednesday.
US	NASA discovered a Y2K fault in planning software for the NASA Upper Atmospheric Research Satellite
US	National Weather Service river gauges failure
US	Netscape's Hitometer has Leap Day bug that effects the whole week
US	On Saturday morning, the e-mail system in the public affairs office and several other offices of the US Census Bureau went out.
US	On Saturday, January 1st, HUD users attempting to use the mortgage termination function in FHA Connection received an incorrect date and an error message and users were temporarily unable to use this particular function
US	One in four IT professionals say their companies have suffered Y2K-related problems since New Year's Eve, according to the survey of 3,243 respondents, including 2,083 IT professionals
US	One of Nordstrom's internal sales tracking systems disabled
US	Pharmaceutical firm was not able to view its data warehouse of inventory and customers
US	Quickbooks Pro 99 malfunction
US	Readers Digest Contest for the new Millennium.. Address label was dated Jan 1900
US	Rite Aid Pharmacy prescription system failure
US	Rite-Aid computer systems failures
US	School software still being checked
US	SeaNet ISP billing system malfunctioned
US	SMS Patient Management systems reported failures in Western United States.
US	Some computer users around the nation who use AT&T's Global Network were unable to access the Internet on Friday night
US	Southern New England Telephone (SNET) bills in error
US	The Carnival Cruise Lines ship Destiny was adrift Tuesday near the Turks and Caicos Islands because of an electrical problem.
US	The city of Grande Prairie will be sending out the first batch of bills after the millennium bug caused a glitch in the system.
US	The Shuttle astronauts encountered one other problem Sunday, this one involving Y2K
US	Thermostat malfunctions at Gold-plating facility
US	U.S. Government sources say there is no indication that the crash of an important computer system at the National Security Agency was caused by Y2K problems.
US	US National Archives have lost an estimated 43,000 e-mails between June 18-21, 1999
US	US National Weather Service website had problem
US	US Postal Service reported a small number of automated retail scales malfunctioned
US	US West telephone equipment failed
US	Using payment software ICVERIFY, NetVERIFY, PCVERIFY and EZCharge must upgrade to Y2K compliant versions to avoid problems
US	Using Quicken 6 for keeping up with personal finances,
US	Visiosonic PHAT MP3 player DLL file expired
US	Window on Wall Street Professional Investor version 5.0 software failure
US	Wind-shear alert systems at the airports in Orlando, Tampa, Denver, St. Louis and Chicago flashed an error message Friday at 7 p.m. when the air-traffic control system switched to year 2000 in Greenwich Mean Time.
US	Wood products manufacturing plant computer failures
US	Yahoo finance website experiencing problems
US	Air Force Y2K Center: almost 40 Y2K glitches by 1/3/00; 10% were mission impact
US - Alabama	Between 15,000 and 20,000 Daphne police and court records dating back to 1992 are inaccessible by computer because of a total system crash.
US - Alabama	Birmingham airport telephone systems malfunctioned
US - Alabama	Computer bug struck Alabama's largest health insurer - Blue Cross and Blue Shield of Alabama
US - Alabama	Huntsville AL NASA facility payroll accounting system malfunctioned
US - Alabama	In December, Daphne mailed some 3,000 water, sewer and natural gas to customers showing the late-payment due date as Jan. 7, 1999.
US - Alabama	The NASA Marshall Space Flight Center will no longer support the production and maintenance of the science.nasa.gov site
US - Alaska	Community of Ivanof Bay in Alaska had problem with the sensors on the day tank of the village power plant
US - Alaska	Golden Valley Electric Association officials still aren't sure what caused a power line south of Healy to trip on Monday evening, triggering two power outages.

Country	Y2K Glitch
US - Alaska	State child support computer system malfunctioned
US - Arkansas	22 counties in Arkansas computer systems malfunctioning
US - Arkansas	Conway County (Arkansas) courthouse computer system software applications failed
US - Arkansas	Jefferson County Treasurer Elizabeth Rinchuso confirmed there has been a minor problem with their computers, but the problem was not Y2K-related.
US - California	A sewer main ruptured at the Buena Vista Pump Station early yesterday, sending 198,000 gallons of sewage into Buena Vista Creek in south Oceanside.
US - California	An emergency siren system used to notify residents of a collapse at Casitas Dam malfunctioned during testing Saturday and instead issued warnings to flee to higher ground.
US - California	Chevron reportedly had a power "interruption" over the weekend, and a spokesman said extra gas passed through the safety flare at its El Segundo, Calif., refinery. Sources said Exxon Mobil's Torrance refinery also experienced a power disturbance over the weekend.
US - California	City accounting program not Y2K-compliant
US - California	LA times has a date of October 17 1999 on top and January 17. 2000 in article.
US - California	Livingston, CA accounting system failure
US - California	Mistakes continue to plague payrolls, Employee tax forms Oakland's latest woe
US - California	NASA's X-38 Crew Return Vehicle test was called off on Feb. 26 when a problem with the vehicle's computers arose
US - California	Legacy system modifications failed
US - California	Palo Nuclear Power plant shut down due to a drop in pressure.
US - California	Port cargo discharge monitoring computer malfunctioned
US - California	power outage on Friday, January 7 at about 4:30 which affected the area near Moorpark and Janss Roads, Ventura County, CA
US - California	Prescription coverage problem in California
US - California	Sacramento Teacher retirement system malfunctioned (STRS)
US - California	San Francisco Automatic Garage Door Corp computer system failed
US - California	San Francisco BART experienced a failure of two systems used for time clocks in their facility
US - California	The Capistrano Unified School District's rankings in the new statewide Academic Performance Index aren't available for public viewing and might not be for some time.
US - California	the electricity went out in Santa Monica Canyon and portions of the Riviera early on January 1 and has been blanking out an average of once a week ever since.
US - California	The failure of an automatic switching system in Oakland threw BART into chaos, creating packed train cars, jamming station platforms and adding traffic to already congested East Bay freeways during the morning commute.
US - California	The Y2K bug hit CSC hard.
US - California	Tosco oil refinery cited for emissions
US - Colorado	Alamosa, CO Post Office credit card authorization system failed
US - Colorado	Aspen Airport closed at 6:00 PM MST on January 12, 2000
US - Colorado	Denver Airport wind shear detector failed
US - Colorado	The City of Reno's AutoCite parking ticket writers had problems Monday
US - Colorado	The City of Sparks, the problem had to do with automatic assigning of police department case numbers
US - Connecticut	As if ailing U.S. Homecare Inc. didn't have enough of a struggle, the Hartford-based company reported Thursday that Y2K computer software problems could hurt cash flow.
US - Connecticut	Concerns among school employees about late W-2 forms and confusing payroll stubs
US - DC	D.C.'s General Hospital is struggling with a new record-keeping system since September '99, which is deemed "inadequate."
US - DC	DC Fire Department payroll computer
US - DC	Howard denial of computer glitch angers students
US - DC	Lines grew at Reagan National Airport near Washington because some check-in computers failed
US - DC	The District's yearly financial report will be delayed up to 45 days because of persistent problems with a new computerized financial management system.
US - DC	The hefty paychecks mistakenly sent by the District of Columbia school system to a teacher who doesn't work for city schools add to a long list of payroll troubles that have yet to be corrected
US - Delaware	America International Insurance Co. system problems
US - Delaware	Conectiv electric utility billing system malfunctioned
US - Delaware	Gambling machines malfunctioned
US - Florida	A glitch in the Palm Beach County Clerk of Circuit Court computer network is causing mortgage, deed and other files to disappear from the system's index, the clerk's office said on Friday.
US - Florida	A last-minute problem with a critical computer delayed space shuttle Endeavor's launch today on a mission to map a still-unknown planet: our own.
US - Florida	Another glitch hits 911 system in Orange, Florida
US - Florida	Columbia County DOT system malfunctioned
US - Florida	Columbia County police system malfunctioned
US - Florida	Company systems failure

Country	Y2K Glitch
US - Florida	Florida Highway Department computer system malfunctions
US - Florida	For about an hour after midnight, computers at Winter Park Memorial in Orange County couldn't access the statewide system for confirming patients' Medicaid eligibility.
US - Florida	Georgia Pacific propane tank releasing propane
US - Florida	Glitch giving SunPass drivers bad messages about cash balance
US - Florida	Hundreds of Orange county school district employees face a delay in getting their W-2 forms for filing income-tax reports because computer errors created faulty tax information on the forms.
US - Florida	In Jacksonville, two minor computer problems were attributed to the Y2K bug.
US - Florida	Jacksonville Sheriff's office computer system malfunctioned
US - Florida	Orlando Airport wind shear detector failed
US - Florida	Pinellas County, FL paid employees twice
US - Florida	Pompano Beach fire officials say that for several months, they have faced potentially life-threatening tie-ups. A computer-aided dispatch system causes delays between the time calls are received and the time they are relayed to firefighters. In some cases, they don't show up at all.
US - Florida	Rouge Steel Company molten steel vessel exploded.
US - Florida	Seminole Community College encountered a glitch when its new student online registration system didn't work.
US - Florida	Tampa Airport wind shear detector failed
US - Florida	Telecommunications glitches in the Ft. Meyers, Florida area
US - Florida	The computer-aided-dispatch system at the Florida Highway Patrol's Orlando headquarters went down from midnight Friday until almost 5 a.m. Saturday
US - Florida	The new Manatee County Public Works system was spitting out water, sewer and garbage bills with unrelated and incorrect data
US - Florida	Utility bills are finally in the mail for 20,000 Manatee County customers a month late after changes intended as Y2K fixes caused problems.
US - Georgia	A computer at the Georgia Department of Transportation considered Tuesday to be in 1900
US - Georgia	a security system completely failed in an office building here at the rollover, leaving the doors completely unlocked.
US - Georgia	Atlanta Airport wind shear detector failed
US - Georgia	Atlanta Police computer system malfunctioned
US - Georgia	Atlanta, GA. Bureau of Buildings building permit system malfunctioning
US - Georgia	Because of a Y2K compliancy plan gone awry, DeKalb County's computerized inmate lists are on the blink --- and so is the system.
US - Georgia	Georgia tobacco farmers waiting on millions of dollars set aside by the nation's tobacco companies to compensate them for the recent blows to the cigarette industry
US - Georgia	Office Depot in Macon reports runs on software by small business owners
US - Georgia	State officials reported only two Y2K glitches a fingerprint identification system run by the Georgia Bureau of Investigation shut down for an hour and a half Saturday, and a GBI system used for filing crime reports went down for an hour on Friday.
US - Hawaii	System failures disrupted police communications island wide for more than six hours Tuesday night,
US - Idaho	America West Airlines Boeing 737-300 was forced to land in Boise
US - Illinois	A computer that runs an energy-management system at a Federal building in Chicago that suddenly flashed the date Jan. 4, 1980.
US - Illinois	All roughly 8,500 Illicall subscribers have received or will soon receive their January 2000 long-distance statements; however, they appear to be a century old already because of a Y2K glitch.
US - Illinois	All roughly 8,500 Illicall subscribers have received or will soon receive their January 2000 long-distance statements; however, they appear to be a century old already because of a Y2K glitch.
US - Illinois	Chicago Bank electronic Medicare payments system disrupted
US - Illinois	Chicago Board of Trade computer system failed
US - Illinois	Chicago O'Hare Airport wind shear detector failed
US - Illinois	Child-support story takes new twist: Mother with grown kids gets checks
US - Illinois	Federal Reserve Bank of Chicago Federal tax payment system
US - Illinois	in the Belleville (Chicago, IL) area, some automated teller machines weren't working, with some machines spitting out cards without explanation.
US - Illinois	International Multifoods of Chicago business system failed
US - Illinois	Moline, IL airport FAA system failed
US - Illinois	Perry County Sheriff's Department system used to track and bill for delivery of civil lawsuit notifications and subpoenas crashed
US - Illinois	Sears Tower Transformer Out for a Brief Period.
US - Illinois	the Chicago O'Hare Airport People Mover stopped running for a short period of time this morning.
US - Illinois	The energy management system at a Federal building in Chicago displayed the date as Jan. 4, 1980. .
US - Illinois	There was one report in Shiloh that railroad gates went down without reason and stayed down.
US - Illinois	Two other federal buildings in Illinois reported date display problems in their security systems.
US - Indiana	An electrical malfunction at a lift station near the Anderson wastewater treatment plant last week

Country	Y2K Glitch
US - Indiana	Around 1:45 p.m., a circuit at a NIPSCO substation east of Southlake Mall "malfunctioned," causing an automatic shutdown of much of the power grid for at least half an hour, NIPSCO spokesman Tom Stevens said.
US - Indiana	Complete conversion to the new Y2K-compliant computer system is taking longer than expected. And because the conversion couldn't take place during the courts' holiday break, employees had to work part of the second week of the new year without a computer system.
US - Indiana	Indiana BMV vehicle registration system
US - Indiana	Indiana Drivers Licenses computer system failed
US - Indiana	State's new computer system that sorts and distributes child support payments has malfunctioned
US - Indiana	Wastewater plant spills 900,000 gallons of partially treated sewage into the White River, but officials report no environmental problems.
US - Indiana	White River, Indiana - mysterious foam is leaking into the river from an unknown source
US - Iowa	A computer problem that has kept many southeast Iowa county treasurers from being able to issue driver's licenses should be solved by Monday.
US - Iowa	Company (Beloit Corp.'s Crystal Street, Lenox Dale, plant) in bankruptcy says Y2k bug caused late payroll
US - Iowa	Metro Record Police computer loses cases
US - Iowa	Several I.V. pumps found non-compliant, Alegent Health Mercy Hospital, Iowa
US - Iowa	Ticket sales for Iowa's lottery drawings were suspended Thursday because of a software problem
US - Iowa	Washington County Sheriff Yale Jarvis reported that The sheriff's and police departments are experiencing several difficulties.
US - Iowa	West Des Moines water department billing system malfunctioned
US - Kansas	A fire alarm system at the Financial Management Service (FMS) office in Lenexa, Kan., was activated at approximately midnight Jan. 1.
US - Kansas	A lock failed at a Food and Drug Administration leased facility in Kansas.
US - Kansas	Bill Singer, Emergency Communications Center director, will ask the Shawnee County Commission on Thursday to solicit proposals on a new Computer Aided Dispatch system because the current equipment isn't Y2K compliant.
US - Kansas	Some small Kansas businesses have found Y2K's first workweek downright buggy.
US - Kansas	Topeka Police Department's evidence inventory computer system malfunctioned
US - Kentucky	oil spilled from a pipeline that burst Thursday afternoon near the fifth hole of the Southwind Golf Course near Winchester.
US - Louisiana	a natural gas line blew in La. 173 in the Caddo Parish community just north of Shreveport.
US - Louisiana	Motiva's 220,000 bpd Norco, LA refinery shuts down
US - Louisiana	Pennzoil's Shreveport, LA refinery complex has a forced closure
US - Louisiana	The New Orleans RTA St. Charles Avenue streetcars stopped running for almost 12 hours as an unidentified problem kept the cars stalled in their tracks all day Sunday.
US - Maine	A lack of accurate storm forecasting apparently occurred due to glitches in the weather service's (Great Barrington, MA) new computer system.
US - Maryland	A Y2K problem led local businesses to overbill credit card customers a total of more than $100,000
US - Maryland	About 2,000 employees of financially troubled Integrated Health Services Inc. did not get paid as scheduled Friday morning
US - Maryland	Fredrick County election board has refused to use the computer system the state has developed
US - Maryland	Insurance Agency Glitch Cancels Policy (Maryland)
US - Massachusetts	Emergency phones along the Adirondack Northway have been out all year with a Y2K-related problem, and state police don't know when they will be repaired.
US - Massachusetts	More than 3,000 Massachusetts Electric customers, including three public schools, were without power for a few hours late yesterday morning after an unknown glitch knocked out service.
US - Massachusetts	Propane company billing system error
US - Massachusetts	Software used to process data and create reports at the town's wastewater treatment plant has experienced a Y2K failure,
US - Massachusetts	The alarm systems at the John F. Kennedy Federal Building in Boston malfunctioned.
US - Massachusetts	The safety-critical feedwater system at the Millstone 2 nuclear reactor in Waterford, Connecticut has malfunctioned today.
US - Massachusetts	There were Y2K "issues," particularly for some major financial institutions.
US - Michigan	FLINT Still perplexed by problems with the new computer water billing system that have caused frustration across the city, officials want to hire the software's manufacturer to help.
US - Michigan	Flint Township Fire Chief Greg Wright has unplugged the County 911 computers in his fire department headquarters, saying the system is so problem-plagued he'd rather go back to dispatching the old-fashioned way
US - Michigan	GRANDVILLE, City's Y2K calendar marred by errors
US - Michigan	Lansing, MI airport FAA system failed
US - Michigan	Many of Flint's more than 40,000 residential water users have been receiving bills based on estimated use or receiving their bills weeks late because of problems linked to new computer software used for the water billing system.

Country	Y2K Glitch
US - Michigan	North Branch water system computer malfunctioned
US - Michigan	Payroll glitches have put the city of Detroit at odds with its 5,500 police employees and with regulators from the state Department of Consumer and Industry Services
US - Michigan	State of emergency for 911
US - Michigan	Washtenaw County employees continue to receive underpayments and other mistakes in their payroll checks more than a month after a new payroll computer system was installed.
US - Michigan	Washtenaw County payroll system malfunctioned
US - Michigan	Water bills charge erroneous late fees
US - Michigan	A previously undetected Y2K problem has emerged in computers at Detroit Metropolitan Airport
US - Minnesota	A possible glitch in the new billing software used by the City of Pierz
US - Minnesota	Company Warns Doctors of Possible Pacemaker Problem
US - Minnesota	Computer hardware problems led to slow or difficult Internet access Monday for thousands of customers in rural Minnesota.
US - Minnesota	Emergency telephone service was disrupted in parts of the Twin Cities area Saturday morning, keeping 911 calls in several communities from getting through to dispatchers.
US - Mississippi	Some Richland residents were shocked to receive letters in the mail from police about overdue traffic citations.
US - Mississippi	University of Southern Mississippi Continuing Education Department server malfunctioned
US - Mississippi	University of Southern Mississippi, the student administration system failed,
US - Missouri	A new computer system delayed summons issuances in a wrongful death suit
US - Missouri	Computer snafu slows DLs
US - Missouri	H&R Block takes online system down after glitch
US - Missouri	local Conoco Gas and Convenience Store here in Kansas City, MO, could not accept credit cards at the pump and their registers inside the store where all messed up.
US - Missouri	St. Louis Airport wind shear detector failed
US - Montana	A fire burning out of control at Asarco Monday night sent smoke billowing through the streets of East Helena
US - Montana	Long distance telephone service is out in central Montana
US - Montana	Technicians still don't know what caused the computer glitch that knocked out long distance phone service for the past two days to thousands of people living in Big Timber, Melville, Reed Point, Rapelje, Molt and Broadview.
US - Montana	Temporary glitches in the state's new tax computer system may mean Montanans will get their tax refunds two weeks later than usual.
US - Montana	The Asarco Oil Refinery near Helena, Montana exploded during the night, from unknown causes" and area residents have been evacuated
US - Montana	the Montana State Department of Revenue announced this morning that "the new computer system which was installed in early December and fully expected to be performing perfectly by now, is not performing to expectations.
US - Nebraska	A DC-8 United Parcel Service jet was forced to make an emergency landing Friday in western Nebraska
US - Nebraska	An American Airlines flight bound for Los Angeles made an emergency landing here Friday after its right engine lost oil pressure and filled the cabin with smoke. The plane landed safely at 7:05 p.m. at Lincoln Municipal Airport.
US - Nebraska	Minor Y2K glitches in Nebraska
US - Nebraska	Minor Y2K glitches in Nebraska
US - Nebraska	Offutt Air Force Base in Nebraska had problems with computers that track aircraft parts and vehicles
US - Nebraska	Omaha Federal Building Security Systems
US - Nevada	The Tahoe DMV told me I didn't exist. They found a glitch in the system, fixed it quickly and I am now back in the system.
US - New Jersey	Computer files report the Virgin Mary sold 248 properties from 1946 to 1972, including deals with B&E Liquors Inc., the Hungarian Boy Scout Association, Union Carbide Corp. and Clover Leaf cemetery.
US - New Jersey	Managers at the Oyster Creek Nuclear Generating Station were investigating why pumps that recirculate water through the reactor core automatically shut down yesterday morning, triggering a controlled shutdown of the reactor.
US - New Jersey	Operators at Oyster Creek nuclear power plant shut down the reactor yesterday morning after three pumps that re-circulate cooling water through the reactor core lost electricity
US - New Mexico	Computer error bills U. New Mexico students for service fees
US - New Mexico	Glitch Confuses Water Customers. It was a new program that they put in to avoid a Y2K problem, and it's become our Y2K problem
US - New Mexico	Glitch crashed the state's mainframe, snarling driver's license applications at the Motor Vehicle Division and causing problems at a few other state agencies.
US - New York	Customer replaced one account at the Municipal Credit Union in the Bronx with a combination savings account and certificate of deposit.
US - New York	Godiva Chocolate Co. cash registers failed
US - New York	New York systems fixed quickly

Country	Y2K Glitch
US - New York	Retail merchandise billing
US - New York	Small New York village accounting system failed rollover
US - New York	Super Video rental computer system problem
US - New York	the Oswego County Sheriff's Department reported a Y2K glitch.
US - New York	Tully village had a crash of the accounting software
US - New York	When the office of "Promoting Enduring Peace" in New York City was opened for the first time after January 1, several systems would not work
US - North Carolina	About 10 minor computer glitches appeared throughout the Duke University Health System
US - North Dakota	Clay County LEC 911 dispatchers have expressed concern that a new computer system installed last summer has glitches that threaten public safety.
US - Northeast	What is causing the distillate price runups in the Northeast?
US - Ohio	Computerized administration system bought to replace non-Y2k compliant one full of bugs
US - Ohio	About 3,000 water customers in West Akron, Firestone Park, Fairlawn and Mogadore received shut-off notices from the city this week -- even though they were completely paid up on their bills.
US - Ohio	An automatic backup to the central computer complex at the Cleveland Air Route Traffic Control Center failed to activate after the rollover.
US - Ohio	Auto insurance database affected by Y2K
US - Ohio	Computer error caused nearly $2 million in extra payouts
US - Ohio	Department of Mental Health system failed
US - Ohio	Firelands Association of Realtors have problems with computerized house catalog system
US - Ohio	Firestone service center stays stuck in 1999
US - Ohio	Graphical capabilities on the Ohio State University website failed
US - Ohio	Ohio Department of Administrative Services system failed
US - Ohio	Ohio jail locks don't pass real Y2K test.
US - Ohio	Ohio University internet access problems
US - Ohio	On Friday December 31st, a small business owner was issued a new and improved (stand-alone) Y2k-compliant credit card swipe machine. It would not accept Visa, MasterCard, or Discover card. By noon that day, the bank delivered another machine. Now it would accept Visa and MasterCard, but not Discover card.
US - Ohio	On Jan. 18, the county auditor's office cut 1,500 checks to pay a wide variety of county vendors, from day-care providers to attorneys representing indigent clients. The Postal Service picked up most of them from the auditor's mailroom the next day.
US - Ohio	Seneca County Sheriff's office had several malfunctions
US - Ohio	Storage tank holding liquid nitrogen ruptured in Cincinnati, OH
US - Ohio	the Y2K bug last week forced the scheduling equipment for the Sandusky Transit System to shut down
US - Ohio	Thousands of Northeast Ohio students will be getting late report cards because a regional educational system had to be changed to avoid the Y2K threat.
US - Ohio	Toledo airport FAA system failed
US - Oklahoma	Department of Human Services payroll system malfunction
US - Oklahoma	Oklahoma Natural Gas Co. experience a Y2K glitch that affected the scheduling of service orders.
US - Oklahoma	Oklahoma radio station automation system
US - Oklahoma	The state Labor Department will investigate chemical exposure to at least 15 employees of Muskogee Regional Medical Center that occurred in January,
US - Oklahoma	Thousands of state Department of Human Services workers monthly paychecks will be delayed until next week
US - Oregon	About 7,000 Oregon high school students who took the battery of tests required for the certificate of initial mastery as sophomores are still waiting to hear if they passed well into their junior year
US - Oregon	Alessandro's Italian Restaurant and Bar has had numerous credit card overcharges
US - Oregon	First major Y2K glitch found in a Oregon state government system
US - Oregon	Portland-based trucking firm accounting system failed
US - Oregon	The U.S. Forest Service could not access some computer files
US - Oregon	Umatilla Oregon Chemical Storage Depot Emergency Alarm failed
US - Pennsylvania	Commerce Bank of Philadelphia "lost" $4800 deposit.
US - Pennsylvania	Easton Publishing Co. computer system department is finding "new problems introduced by software used to solve Y2K problems."
US - Pennsylvania	Gambling machines malfunctioned
US - Pennsylvania	Hershey said last month that its earnings would be lower than anticipated related to continuing troubles with a new automated ordering and distribution system.
US - Pennsylvania	Jury notification system malfunctioned
US - Pennsylvania	Pennsylvania plumbing supply company billing system malfunctioned
US - Pennsylvania	Sunoco refinery has pipeline problem
US - Pennsylvania	Turnpike toll collection and weigh barrier systems malfunctioned in four turnpike locations
US - Puerto Rico	At least 500,000 residents of SAN JUAN were without water Friday because of a failure the day before at a main pumping station.

Country	Y2K Glitch
US - Rhode Island	In Oakland, payroll problems started last October, when the city used new software to process 5,100 checks--1,200 of which had to be adjusted
US - Rhode Island	Newport Beach school district computer called up parents all night long on Monday to tell them their kids were not in school
US - Rhode Island	R.I. court computer glitch delays some arrests
US - South Carolina	Pentagon's Defense Finance and Accounting Service in Charleston S.C., sending out 230 checks to vendors on Jan. 4 with the year 1900
US - Tennessee	A recent computer program change at Knoxville Utilities Board offices led to a weekend hitch in a computer "loop," affecting several of its computer systems, including the one ordinarily used to handle customers' utility bill inquiries.
US - Tennessee	Computer glitch hampers voting
US - Tennessee	Knox County (TN) system used to track car licenses malfunctioned
US - Tennessee	League of Women voters e-mail system failed
US - Tennessee	Oak Ridge's Y-12 nuclear weapons plant tracking system malfunctioned
US - Tennessee	SEQUOYAH Nuclear Reactor Electrical Fault & Reactor Trip
US - Texas	A gas pipeline burst just north of Boyd in a pasture near Farm Road 730, sending natural gas across the northern quarter of the Wise County town.
US - Texas	Alarms went off at the Dallas airport at 12:21 a.m. Saturday in a building containing flight simulators
US - Texas	Because of extensive billing errors in its new local telephone business, AT&T Corp. is rebating all December long-distance charges for about 100,000 Texas customers.
US - Texas	City overpays elevator bill by $53,998.14--computer glitch blamed
US - Texas	Power and telephone outages - centered in North Dallas- lasted for as long as 12 minutes
US - Texas	San Antonio cellular phone and pager business experienced Y2K-related computer problems Monday
US - Texas	TAR members who have made credit card purchases from TAR during the first week of January should check their credit card statements carefully. Due to
US - Utah	Cache County Sheriff's Office had 2 glitches
US - Utah	USU computer system failing sporadically since Jan. 4, registration and cashier lines as well as
US - Utah	Utah Food Bank in Salt Lake City inventory system failed
US - Virgin Islands	Closure of the motor bureau on the three main islands
US - Virginia	BP-Amoco Yorktown refinery malfunction
US - Virginia	Delta Defense ammunition shop explosion
US - Virginia	For the past several weeks, the Prince George's Extra has not received data from the Prince George's County police for the weekly crime report.
US - Virginia	The Montgomery County, Martinsville and Henry County treasurer's offices has been keeping paper records and using calculators
US - Virginia	Y2K still bugging schools
US - Washington	A Seattle area Internet service provider with 17,000 clients billing system malfunctioned
US - Washington	An Alaska Airlines MD-80 jet heading to Los Angeles returned to Seattle-Tacoma International Airport shortly after takeoff Thursday due to engine problems.
US - Washington	Bellevue WA sent Y2K notice to customers with 1900 date
US - Washington	Boeing noted only seven minor Y2K glitches over the first of January
US - Washington	Clallam Bay Correctional Center perimeter fence system malfunctioned
US - Washington	Minor computer glitches hit fuel cards, police dispatch
US - Washington	Reynolds work-release program in Seattle telephone service was disrupted
US - Washington	University of Washington Medical Center radiation equipment malfunction
US - Washington	Washington State Liquor Control Board computer system malfunctioned
US - Washington	Washington State University Fire Department Emergency Medical Service database failed
US - Washington	Washington state's emergency operations center accidentally sent out a news release about an ``emergency'' at the Umatilla Chemical Depot in Oregon that was intended to be used only in an internal drill, the center said today.
US - West Virginia	Charleston, W.VA. airport FAA system failed
US – Wisconsin	A new computer system is blamed for a foul-up that allows University of Wisconsin-Oshkosh students to stay in school even though their grades are unsatisfactory.
US – Wisconsin	Local news Channel 7 had trouble with their weather reporting system
US – Wisconsin	Milwaukee (WI) County Jail boiler failed
US – Wisconsin	Power knocked out for most of Langlade County on Sunday morning.
US – Wisconsin	Some employees of the Schneider National Trucking attempting to access data using the Feb. 29 date were told by the company computer that the command was invalid
US – Wisconsin	The government listings in the Milwaukee white pages are so riddled with errors that Ameritech Corp. has agreed to reprint that section and hand-deliver it for free to consumers next month.
US – Wisconsin	Wisconsin Public Service Corp. in Green Bay, a record-keeping software program was shut down for the day
Venezuela	Failure detected in a major aluminum manufacturing facilities (temperature monitoring system).

Country	Y2K Glitch
Venezuela	Venezuelan refinery problem pushes refined products up further - PDSVA's Amuay Bay refinery is out of service
Vietnam	Vietnam Ba Ria Vung Tau and Thua Thien Hue province telephone switches rolled to 1900
World	The millennium bug caused reports of 100 "significant" systems failures across the world in January, research shows
World	US Senate, In a wrap-up report prepared for release today, the committee identified more than 250 Y2K glitches in some 75 countries, including a nuclear power system failure in the Ukraine and a handful of 911 system breakdowns in the United States.
World	Websites noting incorrect dates.
World	Y2K glitch can crash some Domino servers, Notes clients
Zambia	Disruption in telecommunications traffic between Zambia and Malawi due to date-related problems.
Zambia	PCs were affected in all the Government Ministries which run in-house built Financial Management package. Both the PCs and the software were non-compliant.
Zanzibar	Transmission difficulties believed to be Year 2000 related.
Zimbabwe	Central Mechanical Equipment Department (CMED) custom-made system crashed.
Zimbabwe	Ruwa reported that a non-compliant server that drives their financial and billing system went down.
Zimbabwe	The City of Harare's financial system failed.

Appendix B – Acronyms

ACERT	Army Computer Emergency Response Team
AF	Air Force
AFCA	Air Force Communications Agency
AFCERT	Air Force Computer Emergency Response Team
AFIWC	Air Force Information Warfare Center
AFMC	Air Force Materiel Command
AFNCC	Air Force Network Control Center
AFRL	Air Force Research Laboratory
AID	Agency for International Development
AMC	Army Materiel Command
ANSI	American National Standards Institute
ASC	Aeronautical Systems Center
ASCE	American Society of Civil Engineers
ASD	Assistant Secretary of Defense
ASSIST	Automated Systems Security Incident Support Team
BAFB	Brooks Air Force Base
BIOS	Basic Input Output System
BITS	Banking Industry Technology Secretariat
C2P	Command and Control Protect
C3I	Command, Control, Communications and Intelligence
C4I	Command, Control, Communications, Computing and Intelligence
CAD	Computer-Aided Design
CAM	Computer-Aided Manufacturing
CCIPS	Computer Crime and Intellectual Property Section
CD-ROM	Compact Disk – Read-Only Memory
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CIAO	Critical Infrastructure Assurance Officer/Office
CINC	Combined Intelligence Center/Commander-in-Chief
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPP	Critical Infrastructure Protection Plan/Program
CISS	Center for Information Security
CJCS	Chairman, Joint Chiefs of Staff
CMM	Capability Maturity Model
COL-CERT	DISA Columbus Computer Emergency Response Team
COOP	Continuity of Operations Plan
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
DACS	Data and Analysis Center for Software
DARPA	Defense Advanced Research Projects Agency

DASD	Deputy Assistant Secretary of Defense
DBMS	Database Management Systems
DDoS	Distributed Denial-of-Service
DE	Hanscom Research Site – Energy Directorate
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIAP	Defense-Wide Information Assurance Program
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DIST	Defense Integrated Support Tools
DLA	Defense Logistics Agency
DNS	Domain Name Service
DoD	Department of Defense
DOE	Department of Energy
DON	Department of the Navy
DoS	Denial-of-Service
DOT	Department of Transportation
DSS	Defense Security Service
E2E	End-to-End
EOW	End-of-Week
EPA	Environmental Protection Agency
ESC	Electronic Systems Center
ESS	Emergency Service Sector
EUR-CERT	DISA Europe Computer Emergency Response Team
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FFIEC	Federal Funded Institutions Examination Council
FIDNet	Federal Intrusion Detection Network
FOIA	Freedom of Information Act
GAO	Government Accounting Office
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GSA	General Services Administration
HAFB	Hanscom Air Force Base
HEO	Air Force Research Laboratory Human Effectiveness Office
HHS	Department of Health and Human Services
HP	Hewlett-Packard
HPC	High Performance Computing
HPCC	High Performance Computing Centers
HQ	Headquarters
HRS	Hanscom Research Site
HUD	Department of Housing and Urban Development

IA	Information Assurance
IAW	Interface Assessment Workshop
ICC	National Y2K Information Coordination Center
ICRS	Information Collection and Reporting System
IDS	Intrusion Detection System
IG	Inspector General
ILU	I Love You (computer virus)
INFOSEC	Information Security
IP	Internet Protocol
IPT	Integrated Process/Product Team
IS	Intelligence and Security
IS	Information System
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITAA	Information Technology Association of America
IT-ISAC	Information Technology Information Sharing and Analysis Center
IV&V	Independent Verification & Validation
IW	Information Warfare
IY2KCC	International Y2K Cooperation Center
JS	Joint Staff
JTF-CND	Joint Task Force-Computer Network Defense
KISS	Keep It Simple, Stupid
LAN	Local Area Network
M&S	Modeling & Simulation
MOA	Memorandum of Agreement
MS	Microsoft
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NAVCIRT	Naval Computer Incident Response Team
NDIA	National Defense Industrial Association
NIPC	National Infrastructure Protection Center
NISP	National Industrial Security Program
NIST	National Institute for Science and Technology
NOC	Network Operations Center
NRC	Nuclear Regulatory Commission
NRIC	Network Reliability and Interoperability Council
NRL	Naval Research Laboratory
NSA	National Security Agency
NSF	National Science Foundation
NSIRC	National Security Incident Response Center
NSS	National Security Systems
NTP	Navy Training Plan
OASD	Office of the Assistant Secretary of Defense
ODUSD(S&T)	Office of the Deputy Under Secretary of Defense (Science & Technology)

OIS	Office of Information Security
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OSD	Office of the Secretary of Defense
PAC-CERT	DISA Pacific Computer Emergency Response Team
PAO	Public Affairs Officer
PC	Personal Computer
PDD	Presidential Decision Directive
PDF	Portable Document Format
PEO	Program Executive Office
PM	Program/Project/Product Manager
POC	Point-of-Contact
PSA	Principle Staff Assistant
PTN	Public Telecommunications Network
S&T	Science & Technology
SACST	Special Assistant for Computer and Software Technologies
SANS	System Administration, Networking and Security
SBA	Small Business Administration
SCADA	Supervisory Control and Data Acquisition
SCOTT-CERT	DISA Scott Computer Emergency Response Team
SecDef	Secretary of Defense
SEI	Software Engineering Institute
SEMATECH	Semiconductor Manufacturing Technology
SSA	Social Security Administration
STAMIS	Standard Army Management Information Systems
T&E	Test & Evaluation
TEMP	Test and Evaluation Master Plan
TTE	Table Top Exercise
URL	Uniform Resource Locator
USAF	United States Air Force
USD(A&T)	Under Secretary of Defense (Acquisition & Technology)
USD(C)	Under Secretary of Defense (Comptroller)
USD(P&R)	Under Secretary of Defense (Personnel & Readiness)
USD(P)	Under Secretary of Defense (Policy)
VA	Department of Veteran Affairs
VS	Hanscom Research Site – Space Vehicles
WPAFB	Wright Patterson Air Force Base
Y2K	Year 2000

Appendix C - Resources

Center for Information Security (CISS)
http://ciss.gsa.gov/

> The Office of Information Security (OIS) provides a broad range of technical security services and information technology solutions. It services client's mission-critical requirements with a highly skilled technical staff specializing in Information Security (INFOSEC), Network Engineering, Systems Integration and Installation, Source Selection and Procurement Planning, Project Management, and follow-on support.
>
> Effective October 1, 2000, the General Service Administration's Federal Technology Service realigned its Office of Information Security into two distinct areas - the Center for Information Security Services and the newly created Office of Information Assurance and Critical Infrastructure Protection.

Command, Control, Communications and Intelligence (C^3I) Home Page
http://www.c3i.osd.mil/
http://www.c3i.osd.mil/org/cio/y2k/y2k_con_plan/index.html

> The purpose of this website is to support the overall mission of the OASD(C3I) through the dissemination of public information related to the missions and responsibilities of this organization. This information is posted on this site to satisfy the information needs or mission objectives of one or more audiences, while taking into account operational security, privacy considerations, and force protection.
>
> While the Y2K site is no longer active, the DoD Y2K Contingency Planning site is still active as of 11 February 2002 (although some of the links in the index may not be).

Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice
http://www.usdoj.gov/criminal/cybercrime/

> The Computer Crime and Intellectual Property Section (CCIPS) attorney staff consists of about two dozen lawyers who focus exclusively on the issues raised by computer and intellectual property crime. Section attorneys advise Federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups. Other areas of expertise possessed by CCIPS attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations, and intellectual property crimes.

Computer Emergency Response Team Coordination Center (CERT/CC)
http://www.cert.org/

> The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise located at the Software Engineering Institute, a Federally funded research and development center operated by Carnegie Mellon University.

Critical Infrastructure Assurance Office (CIAO)
http://www.ciao.gov/

> As of 5 February 2002, many of the sites underneath this URL were still under construction.

Defense Acquisition Deskbook
http://web1.deskbook.osd.mil/default.asp?

> The Defense Acquisition Deskbook is an electronic knowledge presentation system providing the most current acquisition policy for all DoD Services and Agencies.

Defense Information Systems Agency (DISA) Automated Systems Security Incident Support Team (ASSIST)
ftp://ftp.assist.mil/ ***(*.mil sites only!)***

> DISA is the DoD's principle agent for the management of DII and operates an Automated Systems Security Incident Support Team (ASSIST) to identify, analyze, assess and resolve DII Information Assurance vulnerabilities, anomalous activities and penetrations.

Defense Security Service (DSS) Information Assurance Website
http://www.dss.mil/infoas/index.htm

> The Defense Security Service (DSS) Industrial Security Information Assurance Branch is comprised of computer security specialists and computer scientists who support existing Industrial Security programs. This site has been designed to help with all Information System (IS) issues as they relate to the National Industrial Security Program (NISP).

Defense-Wide Information Assurance Program (DIAP)
http://www.c3i.osd.mil/org/sio/ia/diap/

> The DIAP's Mission is to ensure the Department of Defense's vital information resources are secured and protected by unifying / integrating Information Assurance (IA) activities to achieve information superiority.

Department of Defense (DoD) Computer Emergency Response Team (CERT) Online
http://www.cert.mil/
http://www.cert.mil/misc/links.htm

> The purpose of this site is to manage, control, monitor and protect essential elements and applications of the Global Information Grid (GIG) in order to ensure it's availability to support the needs of the National Command Authority, CINCs, Services, Agencies and "THE WARFIGHTER". In addition to other resources, the "links.htm" link provides access to the Army Computer Emergency Response Team (ACERT), the Naval Computer Incident Response Team (NAVCIRT), the Air Force Computer Emergency Response Team (AFCERT), and several Defense Information Systems Agency (DISA) CERTs (COL-CERT; EUR-CERT; PAC-CERT; SCOTT-CERT). Note that, as of 13 February 2002, not all of the links were active.

Department of Defense: Confronting Y2K Homepage
http://www.defenselink.mil/specials/y2k/

> This website was provided as a DoD internal information service by the Information Operations Directorate, American Forces Information Service, Office of the Secretary of Defense Public Affairs. This site also has links to other related Y2K sites, including military and military-related (located at http://www.defenselink.mil/specials/y2k/misc_frelate.htm)
>
> Note that, as of 6 February 2002, not all links may be active or accessible by the general public.

Department of the Navy (DON) Chief Information Officer (CIO) Additional Year 2000 Websites
http://www.doncio.navy.mil/y2k/sites.htm

> Many of these sites, as of 11 February 2002, may require UserID/Password information in order to access.

DoD T&E YEAR 2000 - Related Year 2000 Sites
http://www.jcte.jcs.mil/htdocs/teinfo/dodsites.htm

> These sites were selected for their utility in providing substantive information concerning the Year 2000 Problem as it pertains to Test and Evaluation-related Information systems. Links within this site may or may not still be active as of 11 February 2002.

DoD Test and Evaluation Community – Year 2000 Information
http://www.jcte.jcs.mil/htdocs/teinfo/index.htm

This home page provides information on Defense Test and Evaluation (T&E) community efforts to eliminate or mitigate adverse impacts of the century date change on our T&E systems (automated systems for which we have operations and maintenance responsibility).

Federal Computer Week – Search on Y2K
http://www.fcw.com/searchresults.asp?qu=Y2K&ct=fcw&sh=0

This search, performed on 11 February 2002, yielded 699 "hits" on articles related to Y2K issues, both pre- and post-rollover.

Federal Emergency Management Agency (FEMA) Year 2000 Issues
http://www.fema.gov/y2k/

Site still active as of 7 February 2002.

Federal Financial Institutions Examination Council (FFIEC) Y2K Home Page
http://www.ffiec.gov/y2k/

Describes Year 2000 – Century Date Change Initiatives, including sections on FFIEC member activities; Speeches, statutes and videos; Y2K resources and other sites; and Interagency statements and documents.

GAO Year 2000 Computing Crisis: A Test Guide
http://www.doncio.navy.mil/y2k/GAOTestGuide.pdf

This guide was intended to aid organizations in managing and assessing their Year 2000 testing programs.

Information Technology Association of America (ITAA)
(http://www.itaa.org/)
http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=979672846

The Information Technology Information Sharing and Analysis Center (IT-ISAC) is a not-for-profit corporation serving the information technology industry and established to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. The organization will collect, synthesize, and disseminate information about threats and coordinate the information technology industry's response to such threats.

Information Technology Association of America (ITAA) – InfoSec Home Page
http://www.itaa.org/infosec/

This site contains an extensive amount of information relative to Information Security issues.

International Y2K Cooperation Center (IY2KICC)
http://207.233.128.31/

The IY2KCC was created in February, 1999 under the auspices of the United Nations, with funding from the World Bank. Its mission was to promote increased strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Y2K effects on the global society and economy.

MITRE/ESC Year 2000 Website
http://www.mitre.org/research/y2k/

This Year 2000 (Y2K) information is provided as a public service by the Engineering and Program Management Directorate of the Electronic Systems Center of the Air Force Materiel Command (AFMC/ESC), Hanscom Air Force Base (HAFB), Massachusetts, and maintained by the Information Technologies Directorate of The MITRE Corporation, Bedford, Massachusetts.

National Infrastructure Protection Center (NIPC)
http://www.nipc.gov/

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The mission of the NIPC includes the ability to:

- detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures
- manage computer intrusion investigations
- support law enforcement, counterterrorism, and foreign counterintelligence missions related to cyber-crimes and intrusion
- support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests
- coordinate training for cyber-investigators and infrastructure protectors in Government and the private sector

National Y2K Clearinghouse
http://www.y2k.gov/

This clearinghouse creates a single repository of Y2K information to assist the public, business, academia, Federal, state and local governments in obtaining various Y2K information. It is maintained by the U.S. General Services Administration Office of Government-Wide Policy.

Office of Management and Budget – Year 2000 Computer Bug Links
http://www.whitehouse.gov/omb/inforeg/y2kbug.html

President's Commission on Critical Infrastructure Protection
http://www.ciao.gov/PCCIP/
http://www.ciao.gov/PCCIP/pccip_documents.htm

> The President's Commission on Critical Infrastructure Protection was the first national effort to address the vulnerabilities created in the new information age. The Commission, established in July, 1996 by Presidential Executive Order 13010, was tasked to formulate a comprehensive national strategy for protecting the infrastructures we all depend on from physical and "cyber" threats.

System Administration, Networking and Security (SANS) Institute Resources - The Twenty Most Critical Internet Security Vulnerabilities (Updated)
http://www.sans.org/top20.htm

> The SANS/FBI Top Twenty list is valuable because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws on this list.

The Year 2000 Information Center
http://www.year2000.com/cgi-bin/y2k/year2000.cgi

> A still-active link (as of 6 February 2002) that includes articles, user groups, vendor links, and products to build Y2K awareness.

U.S. Army Materiel Command (AMC) Project Year 2000 Action Plan
http://www.monmouth.army.mil/y2k/amcplan.htm

> The AMC Year 2000 Action Plan provided the policy framework and operational direction for HQAMC staff and subordinate activities to use in achieving change of century compliance of all information resources and technology.

U.S. Army Materiel Command Y2K Home Page
http://www.monmouth.army.mil/y2k/y2khome.htm

> Compliance information is located at
> http://www.monmouth.army.mil/y2k/comply.htm

U.S. Army Program Executive Office Standard Army Management Information Systems (PEO STAMIS) Year 2000 Documents
http://www.peostamis.belvoir.army.mil/Y2K/Y2KP4100.htm

U.S. General Accounting Office (GAO) – Special Collections (Terrorism)
http://www.gao.gov/terrorism.html

> Links to full or abstracted GAO reports dealing with various issues of terrorism, including information assurance and critical infrastructure protection.

USAF Year 2000 Home Page
http://year2000.af.mil

Must have .mil or .gov address to access AFCA at Scott AFB. Could not verify whether link was still active as of 6 February 2002.

Y2K-Status.org
http://www.y2k-status.org/Notes/Y2K/

The fundamental premise of this site was that a clear view of the worldwide effort would benefit society as a whole. Only "essential" sites were posted here. Note that the site contains links to DoD, the services, and National Security Y2K resources. Some links may no longer be active, and some may require registration and a UserID/password to access.

Year 2000 Challenge: Department of the Navy – Chief Information Officer (DON CIO)
http://www.doncio.navy.mil/y2k/year2000.htm

Year 2000 International Security Dimension Project – U.S. Navy War College
http://www.nwc.navy.mil/y2k/default.htm

The Year 2000 International Security Dimension Project ran from 1 September 1998 through 28 December 1999. In the fall of 1998, the website was created to facilitate the dissemination of read-ahead packages to participants attending the four workshops that were held (starting in December 1998 and concluding in early May 1999). Once the site was up and running, it became the War College's main portal of interaction with the outside world, reaching a high point in the summer of 1999 when the project's Final Report was posted in late July. From that point on, no more substantive material was added to the site.

Having delivered its last briefing to the outside world on 8 December 1999, it was decided to maintain the original website "as is" for historical archiving purposes and as an example of the sort of decision scenario planning pursued by the Department of the Navy.

Year 2000 Press Clippings
http://www.year2000.com/articles/articles_2001_2.html

This page contains links to online news stories related to Year 2000 computing issues. It contains archived articles (some of whose links may no longer work) from November 1996 through February 2001. After the Y2K rollover, the focus of the articles gradually shifted to Internet security issues (hackers, viruses and worms).

Appendix D - References

"2001 Industry Survey", Information Security, October 2001, http://www.infosecuritymag.com/articles/october01/images/survey.pdf (Link active as of 8 March 2002)

"Air Force Materiel Command Year 2000 Program Management Plan", HQ AFMC, Version 7.0, 7 October 1998

"Air Force Research Laboratory Hanscom Research Site (HRS) Contingency Plan", Department of the Air Force, Air Force Research Laboratory, Hanscom Research Site, 1 October 1998

"Air Force Research Laboratory Hanscom Research Site (HRS) Energy Directorate (DE) and Space Vehicles (VS) Contingency Plan", Department of the Air Force, Air Force Research Laboratory, Hanscom Research Site, 1 September 1998

"Air Force Research Laboratory Hanscom Research Site (HRS) Operational Contingency Plan for Y2K for the Human Effectiveness Directorate at WPAFB", Department of the Air Force, Air Force Research Laboratory Human Effectiveness Office (HEO), 26 October 1998

"Air Force Research Laboratory Hanscom Research Site (HRS) Operational Contingency Plan for Y2K for the Human Effectiveness Directorate at BAFB", Department of the Air Force, Air Force Research Laboratory Human Effectiveness Office (HEO), 26 October 1998

"Air Force Research Laboratory Hanscom Research Site (HRS) Operational Contingency Plan for Y2K for the Propulsion Directorate at WPAFB", Department of the Air Force, Air Force Research Laboratory Human Effectiveness Office (HEO), 20 October 1998

"Air Force Research Laboratory Hanscom Research Site (HRS) Year 2000 Continuity of Operations Plan", Hanscom Research Site (HRS) Contingency Plan, AFRL Y2K Program Management Office, 30 October 1998

"Application of Year 2000 Lessons Learned", Office of the Inspector General, Department of Defense, Report No. D-2001-175, 22 August 2001, http://www.dodig.osd.mil/audit/reports/fy01/01-175.pdf (Link active as of 8 February 2002)

"Assessment of the Year 2000 Problem on Critical Infrastructures", Report to the President's Commission on Critical Infrastructure Protection, 1997, http://www.ciao.gov/PCCIP/Year2000.pdf (Link active as of 15 February 2002)

"Benefits Derived From Organizations' Y2K Preparations", Center for Y2K & Society, http://www.y2kcenter.org/Y2Kbenefits.html (Link became inactive sometime after 18 May 2001)

"Bennett Urges Preservation of Information Coordination Center", Special Committee on the Year 2000 Technology Problem of the United States Senate, 28 February 2000, http://www.senate.gov/~y2k/news/pr20000228.htm (Link active as of 8 February 2002)

"Best Practices and Lessons Learned", National Y2K Information Coordination Center, 19 June 2000, http://www.y2k.gov/docs/ICClesslearn.html (Link active as of 7 February 2002)

"Computer Security Report Card, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, 9 November 2001 http://www.house.gov/reform/gefmir/hearings/2001hearings/1109_computer_security/report_card_blackwhite.xls (Link active as of 5 February 2002)

"Computer Security: How Vulnerable Are Federal Computers?", Committee on Government Reform, Subcommittee on Government Management, Information and Technology, 11 September 2000, http://www.house.gov/reform/gmit/hearings/2000hearings/000911computersecurity/000911sh.htm (Link active as of 5 February 2002)

"Critical Foundations: Protecting America's Infrastructures", Final Report of the President's Commission on Critical Infrastructure Protection, October 1997, http://www.ciao.gov/PCCIP/PCCIP_Report.pdf (Link active as of 15 February 2002)

"Critical Infrastructure Information Security Act of 2001", 107th Congress, 1st Session, Bill # S.1456, 24 September 2001, http://www.senate.gov/~bennett/s1456.html (Link active as of 11 February 2002)

"Critical Infrastructure Protection in the Information Age", Executive Order #13231, 16 October 2001, http://www.ncs.gov/Image-Files/eo-13231.htm (Link active as of 11 February 2002)

"Critical Infrastructure Protection in the Information Age", Presidential Executive Order, 16 October 2001, http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html (Link active as of 8 February 2002)

"Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences"; Report to the Chairman, Special Committee on the Year 2000 Technology Problem; U.S. General Accounting Office Report GAO/AIMD-00-01; October 1999; http://y2k.senate.gov/documents/991004crit.pdf (Link active as of 8 February 2002)

"Defense Computers: Management Controls Are Critical to Effective Year 2000 Testing"; Report to the Chairman, Subcommittee on Defense, Committee on Appropriations, House of Representatives; U.S. General Accounting Office Report GAO/AIMD-99-172; June 1999; http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai99172.pdf&directory=/diskb/wais/data/gao (Link active as of 7 February 2002)

"Defense Computers: Year 2000 Computer Problems Threaten DoD Operations"; Report to Congressional Requestors; U.S. General Accounting Office Report GAO/AIMD-98-72; April 1998, http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai98072.pdf&directory=/diskb/wais/data/gao (Link active as of 7 February 2002)

"Defense Issues Final Status Report on Y2K Preparations", U.S. Department of Defense News Release, Defense*Link*, 16 December 1999, http://www.defenselink.mil/news/Dec1999/b12161999_bt571-99.html (Link active as of 8 February 2002)

"Department of Defense Year 2000 Management Plan", September 1999, http://www.doncio.navy.mil/y2k/Y2KManagementPlan.pdf (Link active as of 6 February 2002)

"Department of the Navy Year 2000 Action Plan", September 1998, http://www.doncio.navy.mil/y2k/DON_Action_Plan.doc (Link active as of 6 February 2002)

"DoD Communications Functional Y2K Master Plan", U.S. Department of Defense, 15 December 1998, http://www.doncio.navy.mil/y2k/CommY2KTestPlanv315Dec98.doc (Link active as of 11 February 2002)

"DoD Critical Infrastructure Protection Execution Plan – Calendar Year 2000", Critical Infrastructure Protection Integration Staff, 13 March 2000, http://ftp.die.net/mirror/cryptome/dodcip/dod031300.doc (Link active as of 8 February 2002)

"Executive Order 13010 – Critical Infrastructure Protection", President of the United States, 15 July 1996, http://www.ciao.gov/PCCIP/eo13010.pdf (Link active as of 15 February 2002)

"First Report Card on Computer Security at Federal Departments and Agencies", Committee on Government Reform, Subcommittee on Government Management, Information and Technology, 11 September 2000, http://www.house.gov/reform/gmit/hearings/2000hearings/000911computersecurity/000911reportcard.htm (Link active as of 5 February 2002)

"FY 2001 Report to Congress on Federal Government Information Security Reform", Office of Management and Budget, 13 February 2002, http://www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf (Link active as of 5 March 2002)

"House Committee Gives Failing Grades to Government Agencies on Computer Security", Tech Law Journal, 12 September 2000, http://www.techlawjournal.com/security/20000912.asp (Link active as of 5 February 2002)

"Information Security – Computer Attacks at Department of Defense Pose Increasing Risks", Electronic Privacy Information Center, May 1996, http://www.epic.org/security/GAO_DOD_security.html (Link active as of 5 February 2002)

"Information Security Management: Learning From Leading Organizations", General Accounting Office, GAO/AIMD-98-68, May 1998, http://www.gao.gov/special.pubs/ai9868.pdf (Link active as of 11 March 2002)

"Information Security: Computer Attacks at Department of Defense Pose Increasing Risks", Report to Congressional Requestors, General Accounting Office, GAO/AIMD-96-84, May 1996, http://www.ja.net/CERT/USA_GAO/GAO-AIMD-96-84/ai96084.txt.pdf (Link active as of 11 March 2002)

"Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies", Report to the Chairman, Subcommittee on Government Management, Innovation and Technology, Committee on Government Reform, House of Representatives; U.S. General Accounting Office Report GAO/AIMD-00-295; September 2000; http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00295.pdf&directory=/diskb/wais/data/gao (Link active as of 7 February 2002)

"International Y2K Glitch Report", International Y2K Cooperation Center, http://207.233.128.31/Glitches2000.htm (Link active as of 11 February 2002)

"Investigating the Year 2000 Problem: The 100 Day Report", United States Senate Special Committee on the Year 2000 Technology Problem, 22 September 1999, http://www.senate.gov/~y2k/documents/100dayrpt/ (Link active as of 6 February 2002)

"Lessons Learned from Army, Navy, Air Force Y2K Projects", Y2K-Status.org, http://www.y2k-status.org/Notes/Y2K/defense/LessonsLearned.htm (Link active as of 6 February 2002).

"Lessons Learned from the Y2K Experience", Emergency Service Sector (ESS) Working Group, 8 February 2000, http://www.fema.gov/nwz00/essy2kreportb.htm (Link active as of 7 February 2002)

"Lessons Learned from the Year 2000 Project", Federal Financial Institutions Examination Council (FFIEC), 21 March 2000, http://www.ffiec.gov/y2k_lessons_learned.htm (Link active as of 11 February 2002)

"Leveraging Y2K Efforts for the Federal Government", Booz-Allen & Hamilton, Impact, Vol. 3, No. 2, June/July 2000, (Link no longer active)

"National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue", Office of the President, 10 January 2000, http://www.ciao.gov/CIAO_Document_Library/national_plan%20_final.pdf (Link active as of 8 February 2002)

"NATIONAL Y2K INFORMATION AND COORDINATION CENTER: Best Practices and Lessons Learned, 19 June 2000, http://www.y2k.gov/docs/ICClesslearn.html (Link active as of 5 February 2002)

"Naval Research Laboratory (NRL) Year 2000 Action Plan - Draft", Naval Research Laboratory, July 1998

"Naval Research Laboratory (NRL) Year 2000 Action Plan - Final", Naval Research Laboratory, September 1998

"Naval Research Laboratory (NRL) Year 2000 Certification and Contingency Plans", Naval Research Laboratory, 20 October 1998

"Naval Research Laboratory (NRL) Year 2000 Financial Management Compliancy", Naval Research Laboratory, 20 October 1998

"Naval Research Laboratory (NRL) Year 2000 Infrastructure Compliancy", Naval Research Laboratory, 20 October 1998

"Naval Research Laboratory (NRL) Year 2000 System Compliancy Database", Naval Research Laboratory, 19 October 1998

"OFFICE OF TREASURY REINVENTION: Year 2000 Lessons Learned", U.S. Customs Service, http://www.y2k.gov/docs/ll/tresuryll.html (Link active as of 5 February 2002)

"Presidential Decision Directive 63: Critical Infrastructure Protection", The White House, 22 May 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (Link active as of 11 February 2002)

"Protecting America's Critical Infrastructures: PDD 63 Fact Sheet", Office of the Press Secretary, The White House, 22 May 1998, http://www.fas.org/irp/offdocs/pdd-63.htm (Link active as of 11 February 2002)

"Report Card: Year 2000 Progress for Federal Departments and Agencies", Committee on Government Reform, Subcommittee on Government Management, Information and Technology, 22 November 1999, http://www.house.gov/reform/gmit/y2k/report_card_final1.pdf (Link active as of 5 February 2002)

"Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities", January 2001, http://www.ciao.gov/CIAO_Document_Library/final.pdf (Link active as of 8 February 2002)

"Senate Y2K Report on DoD - Feb 24, 1999", U.S. Senate, 24 February 1999, http://www.y2k-status.org/Notes/Y2K/defense/SenateReport19990224.htm (Link active as of 11 February 2002)

"Summary of DoD Year 2000 Issues IV", Office of the Inspector General, Department of Defense, Report No. D-2000-057, 16 December 1999, http://www.dodig.osd.mil/audit/reports/fy00/00-057.pdf (Link active as of 7 February 2002)

"Survey 2000: Security Focused", Information Security, September 2000, http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf (Link active as of 5 February 2002)

"Technology Collection Trends in the U.S. Defense Industry", U.S. Defense Security Service, Vol. VII, 2001, http://www.dss.mil/cithreats/2001_trend.pdf (Link active as of 8 February 2002)

"The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 – White Paper", http://www.fas.org/irp/offdocs/paper598.htm (Link active as of 11 February 2002)

"The Department of Defense Critical Infrastructure Protection (CIP) Plan: A Plan in Response to Presidential Decision Directive 63 'Critical Infrastructure Protection'", DASD (Security and Information Operations), Critical Infrastructure Protection Directorate, 18 November 1998, http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm (Link active as of 11 February 2002)

"The Journey to Y2K", Final Report of the President's Council on Year 2000 Conversion, http://www.fema.gov/y2k/lastrep3.doc (Link active as of 7 February 2002)

"The Many Silver Linings of the Year 2000 Challenges", Intergovernmental Advisory Board, U.S. General Services Administration, January 2000, http://www.gsa.gov/Portal/content/offerings_content.jsp?contentOID=114859&contentType=1004&PMGZ=1&S201=1 (Online copy apparently no longer available)

"The Y2K Problem", Statement by John Hamre, Deputy Secretary of Defense, Before the Subcommittee on Government Management, Information and Technology of the Committee on Government Reform and Oversight, 2 March 1999, http://www.house.gov/reform/gmit/hearings/testimony/990302jh.htm (Link active as of 7 February 2002)

"U.S. Army Materiel Command (AMC) Project Year 2000 Action Plan", U.S. Army Materiel Command, http://www.monmouth.army.mil/y2k/act5.doc (Main Document), http://www.monmouth.army.mil/y2k/y2kops.xls (Appendix E) (Links active as of 11 February 2002)

"Y2K Aftermath – Crisis Averted: Final Committee Report", United States Senate Special Committee on the Year 2000 Technology Problem, 29 February 2000, http://www.senate.gov/~y2k/documents/final.pdf (Link active as of 7 February 2002)

"Y2K Center Director Calls Its Closing Lost Opportunity", Government Computer News, 10 July 2000, http://www.gcn.com/vol19_no19/news/2401-1.html (Link active as of 7 February 2002)

"Y2K E2E Contingency Plan", U.S. Army Research Laboratory Major Shared Resource Center, 30 April 1999, Revision 1

"Y2K Experience – Survey Results", TechWeb

http://content.techweb.com/y2ksurvey/results.html
http://content.techweb.com/y2ksurvey/results_p2.html
http://content.techweb.com/y2ksurvey/results_p3.html
http://content.techweb.com/y2ksurvey/results_p4.html
http://content.techweb.com/y2ksurvey/results_p5.html

"Y2K Glitch Report", Hall Associates, http://www.techriskmgt.com/y2k_glitches.xls (Link active as of 6 March 2002)

"Y2K Plus One: Lessons Learned", USA Today Tech Report, 26 December 2000, http://www.usatoday.com/life/cyber/tech/cti942.htm (Link active as of 7 February 2002)

"Y2K: Starting the Century Right", Report of the International Y2K Cooperation Center, February 2000, http://207.233.128.31/February2000Report.pdf (Full Report), http://207.233.128.31/Appendices.pdf (Appendices) (Links active as of 7 February 2002)

"Year 2000 (Y2K) Contingency Plan: Standard Installation/Division Personnel System – 3 (SIDPERS-3)", AISM 25 P04-AAA-ZZZ-Program Management Office-CP, February 2000, http://www.peostamis.belvoir.army.mil/Y2K/Y2KP5000/Y2K32013S.doc (Link active as of 14 February 2002)

"Year 2000 (Y2K) Lessons Learned", A Report to the Congressional Defense Committees, 15 March 2000, http://www.y2k.gov/docs/DODy2klesslearn.pdf (Link active as of 5 February 2002).

"Year 2000 Action Plan", Joint Chiefs of Staff, Version 3.0, February 1999, http://www.dtic.mil/jcs/j6/j6v/JSY2KMGTV3.doc (Link active as of 11 February 2002)

"Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges", Report to the Chairman, Subcommittee on Government Management, Innovation and Technology, Committee on Government Reform, House of Representatives; U.S. General Accounting Office Report GAO/AIMD-00-290; September 2000; http://www.gao.gov/new.items/ai00290.pdf (Link active as of 7 February 2002)

"Year 2000 End-to-End Testing: Logistics Capstone Plan", Department of Defense, Office of the Inspector General, Report No. 00-002, 1 October 1999, http://www.dodig.osd.mil/audit/reports/fy00/00-002.pdf (Link active as of 14 February 2002)

"Year 2000 Lessons Learned: Strategies for Successful Global Project Management", U.S. Department of State, Office of Inspector General, Report No. 01-IT-008, http://oig.state.gov/pdf/y2klessons.pdf (Link active as of 7 February 2002)

"Year 2000 Operational Evaluation Plan", Joint Chiefs of Staff, Version 3.0, March 1999

"Year 2000 Progress for Federal Departments and Agencies", Committee on Government Reform, Subcommittee on Government Management, Information and Technology, 10 September 1999, http://www.house.gov/reform/gmit/y2k/990910gc.PDF (Link active as of 5 February 2002)

"Year 2000 Progress: Quarterly Report as of August 13, 1999", Committee on Government Reform, Subcommittee on Government Management, Information and Technology, 13 August 1999, http://www.house.gov/reform/gmit/y2k/990910sc.pdf (Link active as of 5 February 2002)

"Year 2000 Progress: Quarterly Report as of November 15, 1999", Committee on Government Reform, Subcommittee on Government Management, Information and Technology, 15 November 1999, http://www.house.gov/reform/gmit/y2k/score_card_final1.pdf (Link active as of 5 February 2002)

Anthes, G.H., "Y2K Prophet Comes Down From Soapbox", Computerworld, 10 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO40751,00.html (Link active as of 7 February 2002)

Barrett, R., "Trust Me!: Government and Corporate Infighting Cripples Federal Cybersecurity Efforts", Interactive Week, Vol. 8, No. 32, 20 August 2001, pp. 18-21

Bennett, R.F. and Dodd, C.J., "The Senate Special Report on Y2K: Investigating the Impact of the Year 2000 Problem", Thomas Nelson Publishers, 1999

Bennett, R.F. and Dodd, C.J., "Y2K Aftermath – Crisis Averted, Final Committee Report", The United States Senate Special Committee on the Year 2000 Technology Problem, 29 February 2000, http://www.senate.gov/~bennett/y2kfinalreport.pdf (Link active as of 5 February 2002)

Biggs, M., "New Year's Top 10 List: Lessons That You Should Have Learned from the War on Y2K", InfoWorld, 27 December 1999, http://www.infoworld.com/articles/op/xml/99/12/27/991227opbiggs.xml (Link active as of 7 February 2002)

Braithwaite, T., "Y2K Lessons Learned: A Guide to Better Information Technology Management", John Wiley & Sons, Inc., 2000

Brock, Jr., J.L., "Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination", Testimony Before the Subcommittee on Government Management, Innovation and Technology, Committee on Government Reform, House of Representatives; U.S. General Accounting Office Report GAO/T-AIMD-00-268; 26 July 2000; http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00268t.pdf&directory=/diskb/wais/data/gao (Link active as of 7 February 2002)

Burbano, F., "Year 2000 Computer Problem: Did We Overreact? What Did We Learn?", Testimony Before the House Subcommittee on Government Management, Information and Technology and House Subcommittee on Technology, 27 January 2000, http://www.house.gov/reform/gmit/hearings/2000hearings/000127.y2k/000127fb.htm (Link active as of 6 February 2002)

Burton, T., "Software Configuration Management Helps Solve Year 2000 Change Integration Obstacles", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 7-8, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kobstacles.asp (Link active as of 6 February 2002)

Cohen, B., "ITAA Calls Failing Grade for Fed Cyber Security Unacceptable", Information Technology Association of America (ITAA), 9 November 2001, http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1005327547 (Link active as of 7 February 2002)

Cope, J., "Y2K: Lessons Learned from World-Class Companies", Que Corporation, 1999

Dacey, R.F., "Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets", Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, 9 November 2001, http://www.gao.gov/new.items/d02231t.pdf (Link active as of 8 March 2002)

Date, S., "ITAA Chief Calls for Cybersecurity Facility Modeled on Y2K Center", Government Computer News, 14 August 2000, http://www.gcn.com/vol19_no23/news/2684-1.html (Link active as of 11 February 2002)

Date, S., "Y2K Work is Paying Off", Government Computer News, 31 January 2000, http://www.computeruser.com/newstoday/00/01/31/news1.html (Link active as of 11 February 2002)

Dates, W., "Army Lessons Learned: NDIA – Preparing for Y2K", Presentation to the OSD DISA Y2K Technical Conference, 24 June 1999, http://www.c3i.osd.mil/org/cio/y2k/june99techconf/presentations/15_Dates.ppt (Link active as of 6 February 2002)

Daukantas, P. and Dizard III, W.P., "Walker: Treat Security Like Y2K Effort", Government Computer News, 8 October 2001, pg. 8

Davis, T.M., "Introduction of the Federal Information Policy Act of 2000", Congressional Record, http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?dbname=2000_record&page=E1355&position=all (Link active as of 8 February 2002)

de Jager, P., "Have We Learned Nothing From the Y2K Episode?", Computerworld, 10 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO40594,00.html (Link active as of 7 February 2002)

de Jager, P., "Throwing Down the Year 2000 Gauntlet", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 5-6, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kgauntlet.asp (Link active as of 6 February 2002)

Dean, J., "Feds Get 'F' in Computer Security", GovExec.com, 9 November 2001, http://www.govexec.com/dailyfed/1101/110901j1.htm (Link active as of 5 March 2002)

Dugan, S., "Why We Owe Our Thanks to the Y2K Problem and How We Can Learn Not to Fail Going Forward", InfoWorld, 22 December 1999, http://www.infoworld.com/articles/op/xml/99/12/27/991227opprophet.xml (Link active as of 7 February 2002)

Errington, P., "The Year 2000 Farce", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 25-26, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kfarce.asp (Link active as of 6 February 2002)

Estes, D., "Encapsulation Solutions for Year 2000 Compliance: A Summary", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 9-10, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kencapsulation.asp (Link active as of 6 February 2002)

Estes, D., "Encapsulation Solutions for Year 2000 Compliance: Working Paper", 2000 Technologies Corporation, 1997, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kenc50.doc (Link active as of 6 February 2002)

Federal Acquisition Regulation (FAR) 39, "Acquisition of Information Technology", Part 39.002 - Definitions, http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm#P9_988 (Link active as of 14 February 2002) and Part 39.106 – Year 2000 Compliance, http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm#P52_9963 (Link active as of 14 February 2002)

Garamone, J., "Y2K Has Little Effect on Military Operations", Government Executive Magazine, 3 January 2000, http://www.govexec.com/dailyfed/0100/010300t1.htm (Link active as of 11 February 2002)

Guenier, R., "Y2K – What Really Happened", Taskforce 2000, 26 January 2000, http://www.year2000.com/archive/really.html (Link active as of 7 February 2002)

Hamre, J.J., "Y2K and Frequency Spectrum Reallocation", Statement before the Senate Armed Services Committee Information Systems, 4 June 1998, http://www.fas.org/irp/congress/1998_hr/98060401_ppo.html (Link active as of 11 February 2002)

Harames, P., "Year 2000 Problem Fixes: Don't Hold Out for a Silver Bullet", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 27-29, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2ksham.asp (Link active as of 6 February 2002)

Harris, W.J., "The Challenge of Cyber Threats to the Engineering Profession", ASCE Journal of Infrastructure Systems, Volume 6, No. 2, June, 2000, pp. 53-55

Harrison, A., "Government, Industry Discuss Y2K Lessons", Computerworld, 31 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO40980,00.html (Link active as of 7 February 2002)

Hasson, J., "Y2K Prep Helped Terror Response", Federal Computer Week, 19 October 2001, http://www.fcw.com/fcw/articles/2001/1015/web-y2k-10-19-01.asp (Link active as of 11 February 2002)

Horn, S. and Miller, H., "Agencies Must Step Up Cyberspace Security", Federal Times.com, 19 November 2001, http://www.federaltimes.com/commentary/cio111901.html (Link active as of 5 February 2002)

Jesdanun, A. and Bajak, F., "A Year Later, Lessons from Y2K", MSNBC – Technology, 25 December 2000, (Link no longer active)

Kappelman, L.A., "Lessons Learned from Y2K", InformationWeek 500, 27 September 1999, http://www.informationweek.com/754/kapel2.htm (Link active as of 8 February 2002)

Kappelman, L.A., "Time Spent Fixing Y2K Problems is Yielding Improved and Simplified IT Practices", InformationWeek500, 27 September 1999, http://www.informationweek.com/754/kapel.htm (Link active as of 5 February 2002)

Landers, J., "Government Uses Y2K Lessons in its Blueprint for Cyber-Terror Defenses", Abilene 2000.com, 18 November 1999, http://www.abilene2000.com/wire/lesson1118.html (Link active as of 6 February 2002)

Landers, J., "Y2K Lessons Help Feds Head Off Cyber-Terror", Infowar.com, 30 November 1999, http://www.infowar.com/class_3/99/class3_113099d_j.shtml (Link active as of 7 February 2002)

Lehman, D., "Senate: Y2K Fixes Worth the Billions Spent", Computerworld, 6 March 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO41669,00.html (Link active as of 7 February 2002)

Marro, M., "USAF Y2K Lessons Learned", Presentation to the OSD DISA Y2K Technical Conference, 24 June 1999, http://www.c3i.osd.mil/org/cio/y2k/june99techconf/presentations/17_Marro.ppt (Link active as of 6 February 2002)

McConnell, B., "Y2K Lessons Learned", Federal Computer Week, 7 January 2002, http://www.fcw.com/fcw/articles/2002/0107/mgt-bruce-01-07-02.asp (Link active as of 11 February 2002)

McCormack, J., "The Good, Bad & Downright Ugly", Interactive Week, Vol. 8, No. 34, 3 September 2001, pg. 8

McLaughlin, M., "War on Terrorism Speeds Many Federal IT Plans", Government Computer News, 19 November 2001, pg. 7

Miller, H.N., "The Next Y2K: Protecting the Information Infrastructure of the New Economy", Information Technology Association of America (ITAA), August 1999, http://www.itaa.org/infosec/8-99art.htm (Link active as of 7 February 2002)

Miller, H.N., "Internet Security", Testimony before the Senate Committee on Commerce, Science and Transportation and the Subcommittee on Science, Technology and Space, http://www.itaa.org/infosec/071601testimony.pdf (Link active as of 11 February 2002)

Miller, H.N., "The Computer Security Impact of Y2K: Expanded Risks of Fraud", Testimony before the House Subcommittee on Technology and the Subcommittee on Government Management, Information and Technology, 4 August 1999, http://www.house.gov/science/miller_080499.htm (Link active as of 11 February 2002)

Miller, J., "Davis Plans Services Buying Reform Bill", Government Computer News, 19 November 2001, pg. 7

Murray, B., "Pentagon Y2K Chiefs Land in Industry", Federal Computer Week, 12 January 2001, http://www.fcw.com/fcw/articles/2001/0108/web-dod-01-12-01.asp (Link active as of 11 February 2002)

Newman, C., "Cyber-Security Called 'Dismal'", Washington Post, 12 September 2000, http://www.washingtonpost.com/wp-srv/WPlate/2000-09/12/046l-091200-idx.html (Link active as of 5 February 2002)

O'Hara, C., "Lessons Learned", Federal Computer Week, 10 January 2000, http://www.fcw.com/fcw/articles/2000/0110/Manlessons.asp (Link active as of 11 February 2002)

O'Hara, C., "One Last Y2K Lesson: People Get the Job Done", Federal Computer Week, 21 June 2000, http://www.fcw.com/fcw/articles/2000/0619/web-y2k-06-21-00.asp (Link active as of 7 February 2002)

O'Harrow Jr., R., "Key U.S. Computer Systems Called Vulnerable to Attack", Washtech.com, 27 September 2001, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A32105-2001Sep26 (Link active as of 11 February 2002)

O'Neill, D., "Software Inspections and the Year 2000 Problem", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 17-18, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kinspections.asp (Link active as of 6 February 2002)\

Parker, R.G., "Overblown or Extremely Well Managed? – Solving Year 2000", Information Systems Audit and Control Foundation, http://www.isaca.org/solvingy2k.pdf (Link active as of 7 February 2002)

Pescatore, J., "Computer Security: Cyber Attacks – War Without Borders", Testimony before a Hearing of the Subcommittee on Government Management, Information and Technology, 26 July 2000, http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersecurity/000726jp.htm (Link active as of 11 February 2002)

Porteus, L., "Feds Still Need to Define Role in Tackling Cyberterror, Panelists Say", Government Executive Magazine, 15 May 2001, http://www.govexec.com/dailyfed/0501/051501td.htm (Link active as of 11 February 2002)

Pruitt, S., "16 US Gov't Agencies Flunk Computer Security", IDG News Service\Boston Bureau, 9 November 2001, http://www.idg.net/idgns/2001/11/09/16USGovtAgenciesFlunkComputer.shtml (Link active as of 5 February 2002)

Radcliffe, D., "Y2K's Real Lessons", Computerworld, 10 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO40584,00.html (Link active as of 7 February 2002)

Reed, S.J., "Defense Logistics Agency's Year 2000 Program: Managing Organization-Wide Conversion and Compliance", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 11-16, http://www.stsc.hill.af.mil/crosstalk/1998/jan/dlay2k.asp (Link active as of 6 February 2002)

Rhodes, K.A., "Code Red, Code Red II and SirCam Attacks Highlight Need for Proactive Measures", Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, http://www.gao.gov/new.items/d011073t.pdf (Link active as of 5 February 2002)

Rossheim, J., "Y2K and Beyond: What Have You Really Learned from the IT Project of the Millenium?", Datamation/Earthweb, December 1999, (Link no longer active)

Schaeffer Jr., R.C., "On the Y2K Information Coordination Center (ICC) and How the Lessons Learned Will Apply to the Broader Challenges of Critical Infrastructure Protection", Statement Before the Special Committee of the Year 2000 Technology Problem, 29 July 1999, http://www.defenselink.mil/dodgc/lrs/docs/test99-7-1Schaeffer.rtf (Link active as of 8 February 2002)

Seffers, G.I., "Y2K May Be Model for Defense", Federal Computer Week, 25 September 2001, http://www.fcw.com/fcw/articles/2001/0924/web-home-09-25-01.asp (Link active as of 11 February 2002)

Sliwa, C., "Y2K Gives Some Admins a Security Education", Computerworld, 1 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO40458,00.html (Link active as of 7 February 2002)

Smith, D.B., Muller, H.A. and Tilley, S.R., "The Year 2000 Problem: Issues and Implications", Software Engineering Institute, Technical Report CMU/SEI-97-TR-002; ESC-TR-97-002, April 1997, http://www.sei.cmu.edu/pub/documents/97.reports/pdf/97tr002.pdf (Link active as of 7 February 2002)

Starr, H.S., "C3I to Support Critical Infrastructure Protection: Preliminary Assessments & Observations", The Mitre Corporation, http://www.dodccrp.org/Proceedings/DOCS/wcd00001/wcd00101.htm (Link active as of 11 February 2002)

Stephens, C., "The Air Force and the Year 2000", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 3-4, http://www.stsc.hill.af.mil/crosstalk/1998/jan/airforcey2.asp (Link active as of 6 February 2002)

Stone, P., "Y2K: Looking Ahead, Looking Back", Air Force News, 20 January 2000, http://www.af.mil/news/Jan2000/n20000120_000088.html (Link active as of 11 February 2002)

Thibodeau, P., "Businesses Eye Y2K Effort as Model for Terrorism Fight", Computerworld, 2 October 2001, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO64396,00.html (Link active as of 7 February 2002)

Trilling, S., "What Can Be Done to Reduce the Threats Posed by Computer Viruses and Works to the Workings of Government?", Testimony before the House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, 29 August 2001, http://www.house.gov/reform/gefmir/hearings/2001hearings/0829_computer_security/0829_trilling.htm (Link active as of 5 March 2002)

Tritak, J.S., "Critical Infrastructure Protection: Who's in Charge?", Statement Before the Senate Committee on Governmental Affairs, 4 October 2001, http://www.ciao.gov/News/SenGovAffTritakTmony100401.html (Link active as of 8 February 2002)

Ulrich, W., "Did IT Miss an Important Y2K Lesson?", Computerworld, 3 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO40499,00.html (Link active as of 7 February 2002)

Vaida, B., "Microsoft Security Expert Advocates Rebirth of Y2K Center", Government Executive Magazine, 19 November 2001, http://www.govexec.com/dailyfed/1101/111901td1.htm (Link active as of 5 February 2002)

Vaida, B., "OMB Orders Agencies to Boost Spending on Computer Security", Government Executive Magazine, 4 December 2001, http://www.govexec.com/dailyfed/1201/120401td1.htm (Link active as of 5 February 2002)

Van Raay, C., "Lessons Learned in Y2K Planning", Western News Online, http://comms.uwo.ca/wnews/00-96/issues/2000/jan13/Y2Kfollow.htm (Link active as of 11 February 2002)

Vatis, M.A., "Cyber Attacks During the War on Terrorism: A Predictive Analysis", Institute for Security Technology Studies at Dartmouth College, 22 September 2001, http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf (Link active as of 4 March 2002)

Verton, D., "Billions Needed for Proper IT Security, Expert Says", Computerworld, 18 October 2001, http://www.computerworld.com/itresources/rcstory/0,4167,STO64886_KEY73,00.html (Link active as of 7 February 2002)

Verton, D., "Y2K Fizzles at DoD Bases in Europe, Middle East", Federal Computer Week, 31 December 1999, http://www.fcw.com/fcw/articles/1999/fcw_12311999_europe.asp (Link active as of 11 February 2002)

Voas, J., "Certifying Year 2000 'Fixes'", Crosstalk, Vol. 11, No. 1, Software Technology Support Center, January 1998, pp. 19-20, http://www.stsc.hill.af.mil/crosstalk/1998/jan/y2kfixes.asp (Link active as of 6 February 2002)

Wennergren, D., "Department of the Navy: Year 2000 Challenge", Presentation to the OSD DISA Y2K Technical Conference, 24 June 1999, http://www.c3i.osd.mil/org/cio/y2k/june99techconf/presentations/16_Wennergren.ppt (Link active as of 6 February 2002)

Willemsen, J.C., "Year 2000 Computing Challenge: Leadership and Partnerships Result in Limited Rollover Disruptions", Testimony Before the Subcommittee on Government Management, Innovation and Technology, Committee on Government Reform, House of Representatives; U.S. General Accounting Office Report GAO/T-AIMD-00-70; 27 January 2000; http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00070t.pdf&directory=/diskb/wais/data/gao (Link active as of 7 February 2002)

Willemssen, J.C., "Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks", Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, http://www.house.gov/reform/gefmir/hearings/2001hearings/0926_computer_security/willemssen_testimony_part2.pdf (Link active as of 5 February 2002)

Wohlwend, H., Gladhart, R., Marsden, M., "Year 2000 Readiness Project: Final Report", International SEMATECH, Technology Transfer # 00043937A-ENG, 28 April 2000, http://www.sematech.org/public/docubase/document/3937aeng.pdf (Link active as of 7 February 2002)

Yourdon, E., "Y2K Success Lessons", Computerworld, 24 January 2000, http://www.computerworld.com/cwi/story/0,1199,NAV47-74_STO40853,00.html (Link active as of 11 February 2002)

Appendix E – GAO Reports "Year 2000 Computing Challenge"

Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges. AIMD-00-290 September 12, 2000.

Year 2000 Computing Challenge: Leadership and Partnerships Result in Limited Rollover Disruptions. T-AIMD-00-70 January 27, 2000.

Year 2000 Computing Challenge: Readiness of FBI's National Instant Criminal Background Check System Can Be Improved. AIMD/GGD-00-49 December 16, 1999.

Year 2000 Computing Challenge: Noteworthy Improvements in Readiness But Vulnerabilities Remain. T-AIMD-00-37 November 4, 1999.

Year 2000 Computing Challenge: Federal Business Continuity and Contingency Plans and Day One Strategies. T-AIMD-00-40 October 29, 1999.

Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls. AIMD-00-24 October 29, 1999.

Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs. T-AIMD-00-39 October 28, 1999.

Year 2000 Computing Challenge: FBI Needs to Complete Business Continuity Plans. AIMD-00-11 October 22, 1999.

Year 2000 Computing Challenge: Compliance Status Information on Biomedical Equipment. T-AIMD-00-26 October 21, 1999.

Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning. T-AIMD-00-25 October 21, 1999.

Year 2000 Computing Challenge: DEA Has Developed Plans and Established Controls for Business Continuity Planning. AIMD-00-8 October 14, 1999.

Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs. T-AIMD-00-9 October 6, 1999.

Year 2000 Computing Challenge: Readiness of USDA High-Impact Programs Improving, But More Action Is Needed. AIMD-99-284 September 30, 1999.

Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues. T-AIMD-99-299 September 27, 1999.

Year 2000 Computing Challenge: Status of the District of Columbia's Efforts to Renovate Systems and Develop Contingency and Continuity Plans. T-AIMD-99-297 September 24, 1999.

Year 2000 Computing Challenge: The District of Columbia Cannot Reliably Track Y2K Costs. T-AIMD-99-298 September 24, 1999.

Year 2000 Computing Challenge: FAA Continues to Make Important Strides, But Vulnerabilities Remain. T-AIMD-99-285 September 9, 1999.

Year 2000 Computing Challenge: SBA Needs to Strengthen Systems Testing to Ensure Readiness. AIMD-99-265 August 27, 1999.

Year 2000 Computing Challenge: Readiness Improving Yet Essential Actions Remain to Ensure Delivery of Critical Services. T-AIMD-99-268 August 17, 1999.

Year 2000 Computing Challenge: Important Progress Made, But Much Work Remains to Avoid Disruption of Critical Services. T-AIMD-99-267 August 14, 1999.

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Ensure Delivery of Critical Services. T-AIMD-99-266 August 13, 1999.

Year 2000 Computing Challenge: Agencies' Reporting of Mission-Critical Classified Systems. AIMD-99-218 August 5, 1999.

Year 2000 Computing Challenge: Federal Efforts to Ensure Continued Delivery of Key State-Administered Benefits. T-AIMD-99-241 July 15, 1999.

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Avoid Disruption of Critical Services. T-AIMD-99-234 July 9, 1999.

Year 2000 Computing Challenge: Readiness Improving Yet Avoiding Disruption of Critical Services Will Require Additional Work. T-AIMD-99-233 July 8, 1999.

Year 2000 Computing Challenge: Readiness Improving But Much Work Remains to Avoid Disruption of Critical Services. T-AIMD-99-232 July 7, 1999.

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance. T-AIMD/GGD-99-221 June 23, 1999.

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications. T-AIMD-99-214 June 22, 1999.

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment. T-AIMD-99-209 June 10, 1999.

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain. T-AIMD-99-197 May 25, 1999.

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning. GGD-99-66 May 24, 1999.

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains. T-AIMD-99-180 May 12, 1999.

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk. T-AIMD-99-179 May 12, 1999.

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System. T-AIMD-99-187 May 12, 1999.

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown. T-AIMD-99-163 April 29, 1999.

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions. T-AIMD-99-144 April 14, 1999.

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain. T-AIMD-99-49 January 20, 1999.

Appendix F – GAO Reports "Year 2000 Computing Crisis"

Year 2000 Computing Crisis: Readiness of the Telecommunications Industry. AIMD-99-293 September 30, 1999.

Year 2000 Computing Crisis: Status of Medicare Providers Unknown. AIMD-99-243 July 28, 1999.

Year 2000 Computing Crisis: Customs Is Making Good Progress. T-AIMD-99-225 June 29, 1999.

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services. AIMD-99-190R June 11, 1999.

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning. AIMD-99-178 May 21, 1999.

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries. AIMD-99-162 May 19, 1999.

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds. AIMD-99-154 April 28, 1999.

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector. T-AIMD-99-160 April 27, 1999.

Year 2000 Computing Crisis: Status of the Water Industry. AIMD-99-151 April 21, 1999.

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services. T-AIMD-99-152 April 20, 1999.

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains to Ensure Delivery of Critical Services. T-AIMD-99-149 April 19, 1999.

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services. T-AIMD-99-136 April 15, 1999.

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services. T-AIMD-99-143 April 13, 1999.

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion. AIMD-99-78 April 9, 1999.

Year 2000 Computing Crisis: Readiness of the Electric Power Industry. AIMD-99-114 April 6, 1999.

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls. AIMD-99-37 March 29, 1999.

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain. T-AIMD/RCED-99-118 March 15, 1999.

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed. T-AIMD-99-101 March 2, 1999.

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services. T-AIMD-99-92 February 26, 1999.

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program. T-AIMD-99-85 February 24, 1999.

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk. T-AIMD-99-89 February 24, 1999.

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs. T-AIMD-99-91 February 24, 1999.

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration. T-AIMD-99-90 February 24, 1999.

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service. T-AIMD-99-86 February 23, 1999.

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule. T-AIMD-99-84 February 19, 1999.

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal with Date Change Problem. RCED/AIMD-99-57 January 29, 1999.

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts. AIMD-99-23 January 27, 1999.

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions. T-AIMD-99-50 January 20, 1999.

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs. AIMD-99-28 November 6, 1998.

Year 2000 Computing Crisis: A Testing Guide. AIMD-10.1.21 November 1, 1998.

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues. AIMD/GGD-99-14 October 22, 1998.

Year 2000 Computing Crisis: Updated Status of Department of Education's Information Systems. T-AIMD-99-8 October 8, 1998.

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring Vital Services Are Not Disrupted. T-AIMD-99-4 October 2, 1998.

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information. T-AIMD-98-310 September 24, 1998.

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown. AIMD-98-240 September 18, 1998.

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain. T-AIMD-98-305 September 17, 1998.

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems, But Challenges Remain. AIMD-98-248 September 17, 1998.

Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk. T-AIMD-98-303 September 17, 1998.

Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems. T-AIMD-98-302 September 17, 1998.

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships. T-AIMD-98-278 September 3, 1998.

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact. T-AIMD-98-277 September 2, 1998.

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks. T-AIMD-98-276 September 1, 1998.

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program. AIMD-98-162 August 28, 1998.

Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain. AIMD-98-237 August 21, 1998.

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships. T-AIMD-98-267 August 19, 1998.

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions. T-AIMD-98-266 August 17, 1998.

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions. T-AIMD-98-262 August 13, 1998.

Year 2000 Computing Crisis: Business Continuity and Contingency Planning. AIMD-10.1.19 August 1, 1998.

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges. AIMD-98-124 July 1, 1998.

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies. T-AIMD-98-218 June 22, 1998.

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown. T-AIMD-98-212 June 16, 1998.

Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress. T-AIMD-98-205 June 10, 1998.

Year 2000 Computing Crisis: A Testing Guide (Exposure Draft). AIMD-10.1.21 June 1, 1998.

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted. T-AIMD-98-167 May 14, 1998.

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs. T-AIMD-98-161 May 7, 1998.

Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships. AIMD-98-85 April 30, 1998.

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations. T-AIMD-98-149 April 22, 1998.

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant. T-AIMD-98-116 March 24, 1998.

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services. T-AIMD-98-117 March 24, 1998.

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant. T-AIMD-98-102 March 18, 1998.

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions. T-AIMD-98-101 March 18, 1998.

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (Exposure Draft). AIMD-10.1.19 March 1, 1998.

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant. T-AIMD-98-73 February 10, 1998.

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures. T-AIMD-98-63 February 4, 1998.

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem. AIMD-98-48 January 7, 1998.

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant. T-AIMD-98-20 October 22, 1997.

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach. T-AIMD-97-173 September 25, 1997.

Year 2000 Computing Crisis: An Assessment Guide. AIMD-10.1.14 September 1, 1997.

Year 2000 Computing Crisis: Time Is Running Out for Federal Agencies to Prepare for the New Millennium. T-AIMD-97-129 July 10, 1997.

Year 2000 Computing Crisis: An Assessment Guide--Exposure Draft. 158206 March 1, 1997.

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now. T-AIMD-97-52 February 27, 1997.

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services. T-AIMD-97-51 February 24, 1997.

Appendix G – GAO Reports "Critical Infrastructure Protection"

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection. GAO-02-24 October 15, 2001.

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. GAO-01-1168T September 26, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T September 12, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-1005T July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-769T May 22, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. GAO-01-323 April 25, 2001.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. T-AIMD-00-268 July 26, 2000.

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. T-AIMD-00-229 June 22, 2000.

Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities. T-AIMD-00-181 May 18, 2000.

Critical Infrastructure Protection: National Plan for Information Systems Protection. AIMD-00-90R February 11, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. T-AIMD-00-72 February 1, 2000.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. T-AIMD-00-7 October 6, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. AIMD-00-1 October 1, 1999.

Appendix H – GAO Reports "Information Security"

Information Security: Additional Actions Needed to Fully Implement Reform Legislation. GAO-02-470T March 6, 2002.

Education Information Security: Improvements Made But Control Weaknesses Remain. GAO-01-1067 September 12, 2001.

Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures. GAO-01-1073T August 29, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-751 August 13, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-1004T August 3, 2001.

Information Security: Weak Controls Place Interior's Financial and Other Data at Risk. GAO-01-615 July 3, 2001.

Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program. GAO-01-307 March 30, 2001.

Information Security: Challenges to Improving DOD's Incident Response Capabilities. GAO-01-341 March 29, 2001.

Information Security: Safeguarding of Data in Excessed Department of Energy Computers. GAO-01-469 March 29, 2001.

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. GAO-01-277 February 26, 2001.

Information Security: IRS Electronic Filing Systems. GAO-01-306 February 16, 2001.

Information Security: Weak Controls Place DC Highway Trust Fund and Other Data at Risk. GAO-01-155 January 31, 2001.

Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies. AIMD-00-295 September 6, 2000.

Information Security: USDA Needs to Implement Its Departmentwide Information Security Plan. AIMD-00-217 August 10, 2000.

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. AIMD-00-215 July 6, 2000.

Information Security: Software Change Controls at the Department of Agriculture. AIMD-00-186R June 30, 2000.

Information Security: Software Change Controls at the Department of Commerce. AIMD-00-187R June 30, 2000.

Information Security: Software Change Controls at the Department of Defense. AIMD-00-188R June 30, 2000.

Information Security: Software Change Controls at the Department of Energy. AIMD-00-189R June 30, 2000.

Information Security: Software Change Controls at the Department of Health and Human Services. AIMD-00-194R June 30, 2000.

Information Security: Software Change Controls at the Department of Housing and Urban Development. AIMD-00-195R June 30, 2000.

Information Security: Software Change Controls at the Department of Justice. AIMD-00-191R June 30, 2000.

Information Security: Software Change Controls at the Department of Labor. AIMD-00-192R June 30, 2000.

Information Security: Software Change Controls at the Department of State. AIMD-00-199R June 30, 2000.

Information Security: Software Change Controls at the Department of the Interior. AIMD-00-190R June 30, 2000.

Information Security: Software Change Controls at the Department of the Treasury. AIMD-00-200R June 30, 2000.

Information Security: Software Change Controls at the Department of Transportation. AIMD-00-193R June 30, 2000.

Information Security: Software Change Controls at the Department of Veterans Affairs. AIMD-00-201R June 30, 2000.

Information Security: Software Change Controls at the National Aeronautics and Space Administration. AIMD-00-196R June 30, 2000.

Information Security: Software Change Controls at the Office of Personnel Management. AIMD-00-197R June 30, 2000.

Information Security: Software Change Controls at the Social Security Administration. AIMD-00-198R June 30, 2000.

Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research. AIMD-00-140 June 9, 2000.

Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements. T-AIMD-00-171 May 10, 2000.

Information Security: Controls Over Software Changes at Federal Agencies. AIMD-00-151R May 4, 2000.

Federal Information Security: Actions Needed to Address Widespread Weaknesses. T-AIMD-00-135 March 29, 2000.

Information Security: Comments on Proposed Government Information Act of 1999. T-AIMD-00-107 March 2, 2000.

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. T-AIMD-00-97 February 17, 2000.

Information Security Risk Assessment: Practices of Leading Organizations. AIMD-00-33 November 1, 1999.

Information Security: SSA's Computer Intrusion Detection Capabilities. AIMD-00-16R October 27, 1999.

Information Security: The Proposed Computer Security Enhancement Act of 1999. T-AIMD-99-302 September 30, 1999.

Information Security: NRC's Computer Intrusion Detection Capabilities. AIMD-99-273R August 27, 1999.

DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk. AIMD-99-107 August 26, 1999.

Information Security: Answers to Posthearing Questions. AIMD-99-272R August 9, 1999.

Information Security Risk Assessment: Practices of Leading Organizations (Exposure Draft). AIMD-99-139 August 1, 1999.

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure. AIMD-99-227 July 30, 1999.

Information Security: Recent Attacks on Federal Websites Underscore Need for Stronger Information Security Management. T-AIMD-99-223 June 24, 1999.

Information Security: Subcommittee Questions Concerning the Melissa Computer Virus. AIMD-99-220R June 18, 1999.

Information Security: Many NASA Missions-Critical Systems Face Serious Risks. AIMD-99-47 May 20, 1999.

Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data. T-AIMD-99-146 April 15, 1999.

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk. AIMD-98-92 September 23, 1998.

Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets. T-AIMD-98-312 September 23, 1998.

Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk. T-AIMD-98-170 May 19, 1998.

Executive Guide: Information Security Management--Learning From Leading Organizations. AIMD-98-68 May 1, 1998.

Information Security: Opportunities for Improved OMB Oversight of Agency Practices. AIMD-96-110 September 24, 1996.

Information Security: Computer Hacker Information Available on the Internet. T-AIMD-96-108 June 5, 1996.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. T-AIMD-96-92 May 22, 1996.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. AIMD-96-84 May 22, 1996.

Appendix I – GAO Reports "Defense Computers"

Defense Computers: U.S. Space Command's Management of Its Year 2000 Operational Testing. AIMD-00-30 November 15, 1999.

Defense Computers: U.S. Transportation Command's Management of Y2K Operational Testing. AIMD-00-21 November 15, 1999.

Defense Computers: DOD Y2K Functional End-to-End Testing Progress and Test Event Management. AIMD-00-12 October 18, 1999.

Defense Computers: Management Controls Are Critical to Effective Year 2000 Testing. AIMD-99-172 June 30, 1999.

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises. AIMD-99-52R January 29, 1999.

Defense Computers: Year 2000 Computer Problems Put Navy Operations at Risk. AIMD-98-150 June 30, 1998.

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program. AIMD-98-53 May 29, 1998.

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations. AIMD-98-72 April 30, 1998.

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight. AIMD-98-35 January 16, 1998.

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success. AIMD-98-7R October 21, 1997.

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues. AIMD-97-149 September 26, 1997.

Defense Computers: SSG Needs to Sustain Year 2000 Progress. AIMD-97-120R August 19, 1997.

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort. AIMD-97-112 August 13, 1997.

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems. AIMD-97-106 August 12, 1997.

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem. AIMD-97-117 August 11, 1997.

Appendix J – GAO Reports "Computer Security"

Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-02-231T November 9, 2001.

Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk. GAO-01-600T April 5, 2001.

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171 December 6, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. T-AIMD-00-330 September 27, 2000.

Computer Security: Critical Federal Operations and Assets Remain at Risk. T-AIMD-00-314 September 11, 2000.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. AIMD-00-232 September 8, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. AIMD-00-252 August 16, 2000.

Computer Security: FAA Is Addressing Personnel Weaknesses, But Further Action Is Required. AIMD-00-169 May 31, 2000.

Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software. AIMD-00-55 December 23, 1999.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. AIMD-00-5 October 4, 1999.

Information Security: The Proposed Computer Security Enhancement Act of 1999. T-AIMD-99-302 September 30, 1999.

Responses to Questions on FAA's Computer Security and Year 2000 Program. AIMD-98-301R September 14, 1998.

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems. T-AIMD-98-251 August 6, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. AIMD-98-155 May 18, 1998.

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations. AIMD-98-145 May 18, 1998.

GSA's Computer Security Guidance. AIMD-93-7R July 19, 1993.

Geological Survey: Computer Security. IMTEC-93-10R December 14, 1992.

Computer Security: DEA's Handling of Sensitive Drug Enforcement and National Security Information Is Inadequate. T-IMTEC-92-24 September 30, 1992.

Computer Security: DEA Is Not Adequately Protecting Sensitive Drug Enforcement Data. IMTEC-92-83 September 22, 1992.

Computer Security: Agencies Reported Having Implemented Most System Security Controls. IMTEC-92-45 April 30, 1992.

Computer Security: DEA Is Not Adequately Protecting National Security Information. IMTEC-92-31 February 19, 1992.

Computer Security: Hackers Penetrate DOD Computer Systems. T-IMTEC-92-5 November 20, 1991.

Financial Markets: Computer Security Controls at Five Stock Exchanges Need Strengthening. IMTEC-91-56 August 28, 1991.

Computer Security Weaknesses at the Department of Justice. T-IMTEC-91-15 June 27, 1991.

Serious Questions Remain About Justice's Management of ADP and Computer Security. T-IMTEC-91-17 June 27, 1991.

Justice Automation: Tighter Computer Security Needed. IMTEC-90-69 July 30, 1990.

Impact of the Government-Wide Computer Security Planning and Review Process. T-IMTEC-90-11 July 10, 1990.

Computer Security: Government-Wide Planning Process Had Limited Impact. IMTEC-90-48 May 10, 1990.

Financial System: Federal Oversight of Computer Security Needs to Be Strengthened. T-IMTEC-90-2 February 21, 1990.

Financial Markets: Tighter Computer Security Needed. IMTEC-90-15 January 5, 1990.